

MCWP 6-22

**Communications
and
Information Systems**



U.S. Marine Corps

PCN: 143 00042 00

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes that will improve it. Recommendations may be sent directly to Commanding General, Marine Corps Combat Development Command, Doctrine Division (C 42), 3300 Russell Road, Suite 318A, Quantico, VA 22134-5021 or by fax to 703-784-2917 (DSN 278-2917) or by E-mail to **smb@doctrine div@mccdc**. Recommendations should include the following information:

- Location of change
 - Publication number and title
 - Current page number
 - Paragraph number (if applicable)
 - Line number
 - Figure or table number (if applicable)
- Nature of change
 - Add, delete
 - Proposed new text, preferably double-spaced and typewritten
- Justification and/or source of change

Additional copies: A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status*. An electronic copy may be obtained from the Doctrine Division, MCCDC, world wide web home page which is found at the following universal reference locator: **<http://www.doctrine.quantico.usmc.mil>**.

Unless otherwise stated, whenever the masculine or feminine gender is used, both men and women are included.

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-1775

16 November 1998

FOREWORD

Marine Corps Warfighting Publication (MCWP) 6-22, *Communications and Information Systems*, presents doctrine, tactics, techniques, and procedures (TTP) for the employment of communications and information systems to support Marine air-ground task force (MAGTF) command and control. It builds on the underlying approach to command and control described in Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control*, and supports the basic warfighting philosophy of the Marine Corps as presented in MCDP 1, *Warfighting*. MCWP 6-22 emphasizes the relationship between effective employment of communications and information systems and effective command and control, which leads ultimately to success on the modern battlefield.

MCWP 6-22 provides guidance to communications and information systems (CIS) personnel (officer and enlisted) in planning, installing, operating, and maintaining communications networks and interfacing information systems to those networks. It also provides guidance for commanders and their staffs, who are the users of MAGTF communications and information systems. MCWP 6-22 does not provide detailed instructions on the use of any single item of equipment or system, but rather provides a broad understanding of how communications and information systems are used to support command and control.

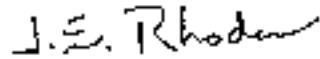
MCWP 6-22 addresses the planning and employment of information systems as well as communications systems. This publication describes the integration of the previously separate functional areas of communications and data processing and emphasizes the rapidly changing nature of information technology and the command and control environment. In this regard, it addresses the impact on the Marine Corps of both the Global Command and Control System (GCCS) and the Defense Information Systems Network (DISN). MCWP 6-22 is intended to be read by all Marines involved in the command and control process, whether as users of information or as operators of communications and information systems.

Substantial developmental efforts are underway throughout the Marine Corps command and control doctrinal hierarchy. The target date for completion of all new and revised command and control series doctrinal publications is the summer of 1999. Pending completion of this task, in the event of terminology, conceptual, operational, or other conflicts between MCWP 6-22 and other FMFM's, MCWP 6-22 takes precedence.

This publication supersedes Fleet Marine Force Manual (FMFM) 3-30, *Communications*, dated 3 April 1989.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

A handwritten signature in black ink, appearing to read "J. E. Rhodes".

J. E. RHODES
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

DISTRIBUTION: 143 000042 00

Communications and Information Systems

Table of Contents

Page

Chapter 1 Command and Control and Communications and Information Systems

1001	Command and Control Environment	1-1
1002	Information Management	1-2
1003	CIS Characteristics	1-6
1004	CIS Responsibilities	1-7

Chapter 2 Organizations

Section I USMC Organizations

2101	Operating Forces	2-1
2102	Marine Corps Forces	2-1
2103	Marine Air-Ground Task Forces	2-2
2104	Marine Corps Forces Reserves	2-4
2105	The Supporting Establishment	2-4

Section II CIS Organizations

2201	Communication Battalion	2-5
2202	Marine Wing Communication Squadron	2-7
2203	Communications Company, HQ Battalion, Marine Division	2-8
2204	Communications Company, HQ and Service Battalion, FSSG	2-8
2205	Communications Platoons, Branches, and Sections	2-9
2206	Special Security Communications Elements and Teams	2-9
2207	Amphibious Squadron Deployment Teams	2-10

Section III C2 Organizations

2301	MEF CE	2-11
2302	Ground Combat Element	2-12
2303	Aviation Combat Element	2-13
2304	CSSE	2-15
2305	Intelligence Command and Control	2-16
2306	Fire Support Centers	2-17
2307	Rear Area Operations Centers	2-17
2308	CIS Control	2-18
2309	Amphibious C2 Facilities	2-20
2310	Mobile CPs	2-21

Chapter 3 Information Systems and Services

Section I Defense Information Infrastructure Common Operating Environment

3101	Mission Applications	3-1
3102	Services	3-1

Section II Global Command and Control System

3201	Background	3-3
3202	Description	3-4
3203	Joint Operation Planning and Execution System	3-4
3204	Global Reconnaissance Information System	3-4
3205	Evacuation System	3-5
3206	Fuel Resources Analysis System	3-5
3207	Global Status of Resources and Training System	3-5
3208	Theater Analysis and Replanning Graphical Execution Toolkit	3-5
3209	Joint Deployable Intelligence Support System (JDISS)	3-5
3210	ATO	3-6
3211	JMCIS	3-6

Section III MAGTF C4I

3301	Migration Strategy	3-7
3302	MAGTF C4I Software Baseline Capabilities	3-7
3303	Hardware/Operating System Requirements	3-7
3304	Maneuver	3-10
3305	Intelligence	3-10
3306	Air Operations	3-12
3307	Fire Support	3-13
3308	Logistics	3-14
3309	Force Deployment Planning	3-15

Section IV The Defense Message System

3401	AUTODIN	3-17
3402	Upgrades	3-17

Section V Information Services

3501	Directory Services	3-18
3502	Terminal Emulation Services	3-18
3503	Message Handling Services	3-18
3504	Network Management Services	3-18
3505	Security Services	3-19
3506	Facsimile Services	3-20
3507	Communications Services	3-20

Section VI Shipboard Information Systems

3601	Key Resources	3-21
3602	JMCIS-Afloat	3-21

Chapter 4 Defense Information Systems Network

4001	Tactical Entry Points	4-1
4002	DISN STEP Services	4-2
4003	STEP Access	4-3
4004	Changes to DISN STEP Sites	4-4
4005	USMC Network Operations Center	4-4

Chapter 5 MAGTF Tactical Communications Network

Section I Overview

5101	Architecture	5-1
5102	Challenges	5-1

Section II Single Channel Radio

5201	HF Radio	5-4
5202	VHF Radio	5-4
5203	UHF Radio	5-5
5204	EPLRS	5-6
5205	UHF-TACSAT	5-6
5206	Commercial International Maritime Satellite	5-8
5207	Data Communications	5-8

Section III Local Area Networks

5301	LAN Media	5-10
5302	LAN Topologies	5-11
5303	Access Methods	5-14

Section IV Switched Backbone

5401	Tri-Services Tactical System	5-16
5402	Switches	5-17
5403	Global Block Numbering Plan	5-21
5404	IP Routers	5-21
5405	Multichannel Radios	5-24

Section V Special Purpose Systems

5501	PLRS	5-35
5502	Precision Lightweight GPS Receiver (PLGR)	5-35
5503	JTIDS	5-35
5504	Integrated Broadcast Services	5-36
5505	Commander's Tactical Terminal	5-36

5506	The Joint Tactical Terminal	5-36
5507	TROJAN SPIRIT II	5-36
5508	Global Broadcast System	5-37
5509	JTF Enabler Module	5-37

Chapter 6 Planning and Execution

Section I Overview

6101	Planning Information	6-2
6102	Coordination	6-2
6103	Security	6-2
6104	Estimates	6-3
6105	Recommendations	6-3
6106	Preparing Plans	6-3
6107	Implementing Plans	6-3

Section II CIS Requirements

6201	Mission	6-4
6202	Courses of Action	6-4
6203	Concept of Operations	6-4
6204	Task Organization	6-4
6205	Available Resources	6-5
6206	Enemy Situation	6-5
6207	Environment	6-6
6208	Information Management Plan	6-6

Section III Pre-Deployment Preparation

6301	Review Existing Plans and Orders	6-8
6302	Prepare Troop and Equipment Lists	6-8
6303	Request Augmentation	6-8
6304	Coordinate Frequencies	6-8
6305	Request Satellite Access	6-8
6306	Compile a Publications Library	6-8
6307	Initiate Telecommunications Service Requests	6-9
6308	Conduct Communications/Command Post Exercises	6-9
6309	Provide CIS Support for Embarkation	6-9
6310	Submit Communications Guard Shifts	6-9
6311	Request COMSEC Material	6-9
6312	Coordinate Logistics	6-9
6313	Effect Liaison/Coordination	6-10

Section IV CIS Plans, Orders, and Directives

6401	Standing Operating Procedure	6-11
6402	CEOI	6-13
6403	CIS Plan	6-14
6404	CIS Estimate	6-14
6405	CIS Concept	6-14

6406	Paragraph 5 of the OPLAN/OPORD	6-15
6407	Annex K (CIS Annex)	6-16
Section V	Communications Control	
6501	Phases	6-17
6502	Responsibilities	6-18
6503	Functional Areas	6-18
Section VI	System Planning and Engineering	
6601	Functions	6-20
6602	Responsibilities	6-20
6603	Automated Tools	6-26
Section VII	SYSCON	
6701	Functions	6-29
6702	Staff Responsibilities	6-29
6703	OSCC Responsibilities	6-31
Section VIII	TECHCON	
6801	Functions	6-32
6802	Responsibilities	6-32
Chapter 7	Information Systems Security	
Section I	Communications Security	
7101	Responsibilities	7-2
7102	Cryptosecurity	7-3
7103	Transmission Security	7-3
7104	Emission Security	7-4
7105	Physical Security	7-4
Section II	Computer Security	
7201	The Threat	7-6
7202	Protection	7-7
Section III	Incident Response	
7301	The Fleet Information Warfare Center	7-9
7302	Naval INFOSEC Help Desk	7-9
7303	The Air Force Information Warfare Center	7-10
7304	Points of Contact	7-10

Chapter 8 Future Directions

8001	Operational Maneuver From the Sea	8-1
8002	CIS Requirements	8-2

Appendices:

A	Defense Information Infrastructure Common Operating Environment Compliance	A-1
B	Common Hardware and Standard Commercial Software Applications	B-1
C	Ship Visit Checklist	C-1
D	MAGTF Radio Nets	D-1
E	Information Systems Directory	E-1
F	CIS Planning Checklist	F-1
G	Unit Planning Checklist	G-1
H	Data Communications Network and Information Systems Planning Checklist	H-1
I	Communications and Information Systems Estimate	I-1
J	Sample CIS Annex (Annex K)	J-1
K	CIS Threat Assessment Planning Checklist	K-1
L	Emission Classification and Designation	L-1
M	Sample Guard Charts	M-1
N	Points of Contact	N-1
O	Glossary	O-1
P	References and Related Publications	P-1

Chapter 1

Command and Control and Communications and Information Systems

MCWP 6-22 outlines the responsibilities of CIS personnel and CIS users to ensure that those systems provide effective command and control (C2) support. MCWP 6-22 is written, to the extent possible, in nontechnical language. However, chapters 3, 4, and 5 contain many computer networking and communications terms that may be unfamiliar to most Marines. These terms are defined in appendix O.

MCWP 6-22 focuses on the CIS used to support the MAGTF in the operational environment. It addresses CIS employment in support of the Marine Corps component headquarters and how the Marine Corps organizes to provide CIS support to the MAGTF. It describes the information systems and services that support MAGTF C2 and the employment of communications systems and networks to link these information systems.

This publication emphasizes the impact of the rapidly evolving joint C2 environment on Marine Corps CIS. Key planning considerations, guidelines, and procedures are presented. CIS operation is then discussed in terms of system planning and engineering, operational systems control (SYSCON), and technical control (TECHCON) followed by information security (INFOSEC) and communications security (COMSEC). MCWP 6-22 concludes with a discussion of future CIS concepts.

1001. Command and Control Environment

The C2 environment is characterized by rapid change and continuous challenge. Implementation of maneuver warfare doctrine, with its emphasis

on speed and tempo, demands compressed planning, decision, execution and assessment cycles. At the same time, the volume of information that needs to be processed and analyzed to support decisionmaking is exploding, and this information overload threatens to overwhelm the commander and his staff. The MAGTF must employ limited CIS resources to meet these challenges. To help satisfy the operational requirement, the Marine Corps is changing its manpower structure and its education and training processes as well as its doctrine through the combat development process. Changes are based on integrating the previously separate functional areas of communications and data processing into a single functional area with responsibilities for both information processing and information exchange. This merger will position the Marine Corps to take full advantage of advances in information technology to meet C2 requirements.

Developments in the joint C2 arena are another significant factor in the C2 environment. The Department of Defense (DOD) is significantly enhancing the C2 capabilities of the armed forces by rapid exploitation of advanced information technologies and significant improvements in interoperability. These accomplishments are largely the result of the implementation of the Defense Information Systems Network (DISN) and the GCCS and the associated Joint Technical Architecture standards. The DISN is an integration of DOD communications systems and networks under the management control of the Defense Information Systems Agency (DISA). The ultimate goal of DISN is to provide a single, integrated, common-user, global communications network that supports all echelons, strategic through tactical. Similarly, the GCCS is designed to replace incompatible Service-unique C2

systems with a single, integrated C2 system. Implementation of GCCS will ensure interoperability among forces and provide a common operational picture and a common set of decision support tools for all components of the joint task force (JTF). Through communications connectivity provided by the DISN, GCCS will support the planning, deployment, employment, sustainment, and redeployment of joint forces worldwide. It will be some years before the DISN and GCCS are fully implemented. However, GCCS and DISN, as discussed in chapters 3 and 4, are already having a major impact on the employment of Marine Corps CIS.

One of the most difficult C2 issues currently facing the Marine Corps is the requirement to support a deployable Marine component HQ with CIS personnel and equipment. The primary source of support is the communications battalion. The requirement to provide support to a deployed Marine component HQ can have a significant effect on the availability of CIS resources to support the MAGTF. Resources required to support a component HQ is the subject of ongoing study and will be addressed by the next Force Structure Planning Group.

CIS must be able to satisfy the C2 requirements of the expeditionary battlefield. CIS must provide MAGTF commanders and their staffs with the tools necessary to rapidly collect, process, analyze, and exchange information in support of operations planning and execution. These systems must make available the information needed, when it is needed, wherever it is needed on the battlefield. Employment of these systems must not adversely affect the freedom of action and mobility of the MAGTF. They must be reliable, flexible, and responsive. The success of the MAGTF on the modern battlefield depends on designing, planning, and employing CIS that satisfy the information needs of the MAGTF C2 process.

1002. Information Management

Much of the information obtained for any endeavor or purpose is contradictory. This is especially

true in a battle of wills between opposing forces in military or political conflicts in which each side seeks to deceive the other with false information. The commander cannot, therefore, be certain that the information obtained depicts the situation with absolute certainty, only that it provides an approximation of reality. Generally, the commander's approximation of reality can be increased with more time to collect and analyze additional information. However, reality also changes with time because of enemy and friendly actions and the environment. These changes then introduce additional information that requires processing and analysis. At some point, the commander must make decisions based on the best information available. Although CIS provide useful tools, the application of sound information management principles is required to satisfy the commander's information requirements.

a. Information Quality

Information quality and availability have a direct effect on the commander's capability to effectively C2 forces. Good information reduces confusion and contributes to situational awareness. Good information is essential for effectively planning, monitoring, and influencing operations. Information quality cannot be taken for granted and must be assessed with care.

The following criteria are by no means all-inclusive, nor are they independent or all of equal importance. It is counterproductive to seek complete information if the search for completeness makes the information untimely. Irrelevant information is worse than no information, and false information can be disastrous, especially if it is part of an enemy deception.

(1) Relevance. Information must apply to the mission, task, or situation. Exhaustive information provided without filtering often detracts from rather than enhances the commander's ability to make timely, effective decisions. Furthermore the transmission and processing of exhaustive information ties up CIS.

(2) Timeliness. Information must be available at the appropriate place and time to be useful. Information management procedures and techniques must ensure the timely, unimpeded flow of relevant information. Well-planned and implemented CIS; clearly identified information requirements; effective collection, reporting, and dissemination; and decisiveness by commanders and staff all contribute to timely information.

(3) Accuracy. Information must be as accurate as possible. Although information systems can collect, transport, process, disseminate, and display information, Marines must still evaluate the information and make decisions as to its accuracy, timeliness, and relevance.

(4) Completeness. Information may be useful only when it is complete. However, by the time complete information is obtained, it may no longer be timely. If subordinates are aware of the commander's intent and critical information requirements, they can provide only those information fragments needed for situational awareness.

(5) Objectivity. Information must be provided in the most undistorted, factual, and unbiased way possible. Any interpretation should be highlighted.

(6) Usability. The display or presentation of information to the user must be understandable and useful. Standard, clearly understandable information formats, symbols, and terms should be used to exchange information and present it to users. Information exchanged and presented in non-standard form causes delays in interpretation and is more easily misunderstood, thereby leading to longer decision and execution cycles and, ultimately, to less reliable decisions.

b. Information Defined

In this publication, the term information refers to all information that is needed to support the decisionmaking process on the battlefield that information required to execute the planning, decision, and execution cycle in combat. Joint Pub 0-2, *Unified Action Armed Forces (UNAAF)*, pro-

vides two definitions for information: (1) facts, data, or instructions in any medium or form, and (2) the meaning that a human assigns to data by means of the known conventions used in their representation. It is important to understand that the term information, in its broadest sense, includes everything from raw data, perhaps a radar signal or a suspected enemy sighting by an observation post, to data that has been extensively processed into useful information for a decision maker. Ultimately, study and analysis of information leads to an understanding of the situation, that is, situational awareness. Navy doctrinal publication (NDP) 6, *Naval Command and Control*, and MCDP 6, *Command and Control*, describe a four-step cognitive process by which the transformation from raw data to situational awareness takes place. (See fig. 1-1 on page 1-4.) These four steps may be viewed as defining an information hierarchy.

(1) Data. The first step in the cognitive process is to collect raw data. The raw data can take many forms: radar signals, intercepted radio signals, meteorological data from a weather balloon, or even bar-coded logistic data scanned from the side of a container. This data may be transmitted in either analog or digital formats by telephone, radio, or facsimile; transferred between computers over local area networks (LANs); or sent by messenger as rolls of undeveloped film or perhaps computer diskettes. In any event, to be useful, this raw data must be processed into a form that can be understood by the ultimate user.

(2) Processed Data. Processing data involves a wide range of functions from decoding and translating intercepted communications to filtering and correlating sensor returns to developing film. Processing includes placing information into a form, such as a graphical display or a formatted message, that can be readily interpreted. Some information will come to the MAGTF in processed form and will not require further processing. Once data has been processed, it is referred to as information in the cognitive process. At this point some information may have immediate value for Marines in close contact with the enemy. Such information is known as *combat*

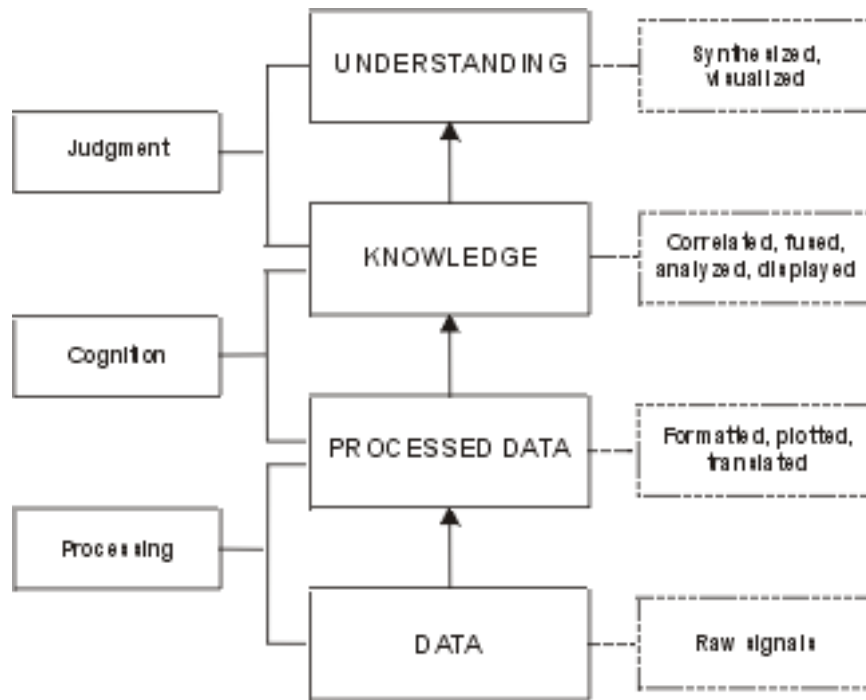


Figure 1-1. Information Hierarchy.

information. It is usually extremely perishable and should be disseminated to using units as rapidly as possible.

(3) Knowledge. In the next step, information is analyzed and evaluated. Through this process of analysis and evaluation comes knowledge. For example, the analysis of intelligence information helps build a picture of the enemy situation.

(4) Understanding. The last step in the process is the development of an understanding of the situation based on the information available. Understanding is the result of applying human judgment based on individual experience, expertise, and intuition to gain a full appreciation of the battlefield. This understanding is situational awareness and provides a sound basis for operational decisions. It allows the commander to anticipate events and to uncover critical vulnerabilities for exploitation. As we strive to gain an understanding of the situation, however, we must recognize that time is working against us. We may not be able to gain complete situational awareness before acting. Developing situational

awareness with limited and uncertain information under severe time constraints is the fundamental C2 challenge.

c. Types of Information and Commander's Critical Information Requirements (CCIRs)

The information required for situational awareness falls into three general categories: information about the enemy, information about the environment, and information about friendly forces. The identification of CCIRs is a means to focus and direct the collection and processing of information in those categories. CCIRs are the information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Designation of CCIRs reduces the volume of information to a manageable level and helps to ensure the accuracy, relevance, and timeliness of that information. CCIRs comprise priority intelligence requirements (PIRs), friendly force information

requirements (FFIRs), and essential elements of friendly information (EEFIs). Clearly defining these information requirements is one of the most difficult and important tasks of command. CCIRs will not only govern the quantity and quality of the information available to support decisionmaking, but also have a direct effect on the workload of the staff and subordinate units.

(1) PIRs. PIRs are intelligence requirements associated with a decision that will affect the overall success of the command's mission. PIRs include both information about the enemy and information about the environment. Information about both enemy capabilities and intentions is critical to allow commanders to anticipate and analyze possible enemy courses of action (COAs). Information on the environment includes information on the weather, the terrain, the local population, the local communications and transportation infrastructures, and a host of other factors that may affect the conduct of military operations. Through identification of PIRs, commanders ensure that limited intelligence resources are directed to obtaining intelligence information that is essential for decisionmaking.

(2) FFIRs. To complete the picture of the situation, the commander requires information on friendly forces. FFIRs are the information the commander needs about friendly forces to be able to develop plans and make effective decisions. Depending on the circumstances, information on unit location, composition, readiness, personnel status, and logistic status could become an FFIR. Just as it is essential for the commander to use PIRs to identify the most important requirements for information on the enemy, it is also essential for the commander to specify what critical friendly information is required to support planning and execution. The commander must have real-time or near real-time information on the location, status, and capabilities of friendly forces. However, FFIRs must be prioritized to limit and focus the collection and processing effort. It is easy to overburden subordinate units, as well as to overload communications networks, with requests for non-essential information. FFIRs help commanders, staffs, and subordinate units understand precisely

what information is needed to support the planning, decision, execution and assessment cycle.

(3) EEFIs. EEFIs are specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. These EEFIs may be viewed as representing the opposing commander's PIRs. Identification of the EEFIs is key to planning effective INFOSEC, operations security, and other force protection operations.

d. Flow of Information

The goal of information management is to facilitate a rapid, unconstrained flow of information throughout an organization from its source through intermediate collection and processing nodes to its delivery to the ultimate user. CCIRs serve as a necessary filter to ensure that only relevant information is delivered, thereby preventing information overload. Information must flow in all directions to support a common picture of the battlefield among all units—senior, subordinate, adjacent, supporting, and supported alike. A flexible, responsive MAGTF C2 architecture is required that pushes relevant, time-sensitive information to the user while allowing the user to pull additional detail as required. This C2 architecture consists of the C2 facilities, information systems, and communications networks that are described in chapters 2, 3, 4, and 5.

A number of networking techniques are widely used to improve the flow of information both within and between Marine Corps organizations. These techniques support improved situational awareness and collaborative planning. Networking also offers tremendous opportunities for "electronic reachback." The concept of electronic reachback may reduce the size of deployed staffs through the use of specialists—military, government civilian, or consultant—who never deploy. The Marine Corps Chemical/Biological Incident Response Force (CBIRF) provides an excellent example of this approach.

The most widely used networking technique is e-mail. E-mail provides a convenient means for

exchanging information between both organizations and individuals and is a highly effective means of communication. E-mail supports rapid dissemination of time-critical information between a HQ and subordinate organizations and across staff sections. Organizational e-mail has replaced much of the information traffic that was previously sent over the Automatic Digital Network (AUTODIN). E-mail permits a single user to disseminate information to one or several users simultaneously. However, in a deployed environment, the potential to overload the communications system requires a disciplined approach to the establishment and use of e-mail accounts.

Other networking techniques support the concept of information pull and have the potential to reduce the load on the communications network and thereby improve the information flow. These techniques include using home pages and newsgroups as well as shared network drives on a LAN. However, posting information to a newsgroup or a home page, or updating a file on a LAN server, is no guarantee of receipt by the intended audience.

Pull techniques are generally unacceptable for the promulgation of time-sensitive critical information such as fragmentary orders or warning orders. Although brief messages could be sent indicating that the order had been posted and requiring addressees to acknowledge and comply, the order itself normally would not have been lengthy enough to make this an efficient approach. On the other hand, when selective access to information in large databases is required to support an analysis, pull techniques are more efficient than push techniques.

1003. CIS Characteristics

It would be impossible to provide adequate C2 support on the modern battlefield without CIS. This publication defines CIS as any system whose primary functions are to collect, process, or exchange information. CIS should be reliable,

secure, timely, flexible, interoperable, and survivable.

a. Reliability

CIS should be available when needed and perform as intended, with low failure rates and few errors. Reliability is also attained by standardizing equipment and procedures, building necessary redundancy, establishing effective logistic support, and protecting against computer viruses, electronic jamming, and deception. Systems should perform reliably aboard ships and aircraft, in garrison, and in austere field environments.

b. Security

CIS should provide security commensurate with the user's requirements and with the vulnerability of the transmission media to interception and exploitation. Security is achieved by using appropriate protection and cryptographic systems, using transmission security techniques, and educating and training personnel in security procedures.

c. Timeliness

CIS should process and transfer information between decision makers rapidly enough to maintain a high tempo of operations and ensure that our decision and execution cycle remains ahead of any potential adversary's.

d. Flexibility

CIS should be capable of being reconfigured quickly to respond to a rapidly changing environment. Flexibility can be obtained through system design or by using commercial facilities, mobile or transportable systems, or prepositioned facilities.

e. Interoperability

CIS should enable information to be exchanged among all of the commanders and forces involved

in an operation. MAGTF CIS also should possess the interoperability required to ensure information exchange in joint and multinational operations and in operations with other Government agencies.

f. Survivability

Survivability is all measures taken to prevent disruption of CIS by enemy interference or natural disaster. Survivability can be enhanced by the dispersal and protection of key nodes, physical and electromagnetic hardening, and redundancy of communications paths and information processing nodes.

1004. CIS Responsibilities

The officer military occupational specialties of 2502, communications officer, and 4002, data processing officer, have been merged into a single military occupational specialty, 0602, CIS officer (CISO). Responsibility for this functional area has been assigned to the G-6/S-6. To reflect this assignment of responsibility, this publication refers to the G-6/S-6 as the CISO, rather than communications officer or communications-electronics officer. Since the technology associated with such systems and networks continue to evolve, specific responsibilities continue to evolve as well. Already it is clear that responsibilities for installing and operating information systems will be shared between CIS specialists and functional area users. For example, the tactical combat operations (TCO) system will be operated by personnel from the G-3/S-3. However, they will be assisted in installing the system and interfacing the system to LANs and wide area networks (WANs) by CIS personnel.

Just as important as the responsibility for installing, operating, and maintaining CIS is the responsibility for the management of the information processed and exchanged by those systems. Each staff section will be responsible for the quality of the information in the databases of the systems that support that particular staff section.

However, overall information management policy and procedures will be under the staff cognizance of the chief of staff (C/S) or the executive officer (XO).

a. Commander

The commander is responsible for the employment of CIS within the command. Although the authority to plan and employ communications and information systems may be delegated, ultimate responsibility for CIS planning and employment remains with the commander. The commander must provide adequate guidance, including necessary assumptions and constraints, to support the development of CIS estimates, plans, and orders. The commander is also responsible for providing the focus for information management throughout the organization and participates directly in the information management process by establishing the CCIRs discussed in paragraph 1002c.

b. Communications and Information Systems Officer

The CISO is responsible to the commander for all matters concerning the planning and employment of CIS within the command. As a general or executive staff officer, the CISO serves as an advisor, planner, supervisor, and coordinator. Specific responsibilities include—

(1) Providing the commander and other staff officers with—

- Advice on information management policies and procedures.
- Estimates of the supportability of courses of action (COAs).
- Estimates of requirements for CIS resources—personnel, equipment, supplies, and facilities.
- Recommendations for the allocation and use of CIS resources.
- Recommendations for CIS training for the command.

- Recommendations on the location, echelonment, and displacement of the command post (CP) and C2 facilities.
- Advice on operational aspects of information systems security (INFOSEC). See chap. 7 for detailed G-6/S-6 responsibilities.

(2) Preparing CIS plans, orders, and standing operating procedures (SOPs) to implement the commander's policies and decisions on CIS employment.

(3) Assisting the staff in the area of CIS for the preparation of studies, estimates, plans, orders, instructions, and reports.

(4) Ensuring compliance with the commander's orders and instructions by supervising—

- Employment of CIS personnel.
- Installation, operation, and maintenance of communications networks.
- LAN and WAN management, including Internet Protocol (IP) address and routing management.
- Technical support for functional users in the installation, operation, and maintenance of information systems hardware and common user software.
- Communications systems training and, in coordination with functional users, information systems training.
- Supply and maintenance of CIS.
- Compliance with SOPs and interoperability standards.
- CIS security in coordination with the other staff sections.

(5) Coordinating CIS matters with cognizant staff sections and with staffs of other units, as required.

(6) Establishing CIS liaison with senior, subordinate, adjacent, supported, and supporting units.

c. Unit Information Management Officer

The unit information management officer is a special staff officer operating under the staff cognizance of the C/S or XO. If an information management officer is not designated, then this duty is the responsibility of the C/S or XO. The information management officer is responsible for establishing the policy and procedures for information management within the command. Responsibilities include:

(1) Coordination, with the assistance of the information management officers of each staff section and subordinate units, of information management efforts throughout the organization.

(2) Development and publication of the information management plan. The information management plan establishes policies and procedures for ensuring the quality and flow of information within the organization.

(3) Coordination of the CCIR process: the nomination of CCIRs; approval of CCIRs by the commander and collection and reporting of CCIRs by the staff; dissemination of CCIRs to higher, adjacent and subordinate commands; and maintenance of CCIRs.

(4) Development and implementation, in close coordination with the CISO and other staff principals and subordinate units' information management officers, of effective information dissemination techniques.

(5) Development of training programs on information management procedures.

(6) Coordination with the unit security manager in the development and implementation of information security procedures.

(7) Coordination with the CISO on LAN management and networking issues, communications channels prioritization, and traffic management.

d. Staff Section Information Management Officer

Each staff section should appoint an information management officer. The staff section information management officer is responsible for—

- (1) Coordinating the internal and external information flow for the staff section and its integration with the information flow of other staff sections, including identifying and prioritizing information management requirements.
- (2) Providing the unit information management officer with input to the information management plan.
- (3) Coordinating information management training for section personnel with the unit information officer.
- (4) Coordinating the identification and processing of all CCIRs within the staff section's area of responsibility (AOR).
- (2) Serving as the configuration manager for information systems supporting the functional area.
- (3) Conducting routine information system administration (assigning user identification, passwords, and privileges; performing data/file storage and management; conducting system backups).
- (4) Coordinating with the G-6/S-6 to ensure that adequate hardware, software, trained personnel, and procedures are in place before implementing a new system or system modification.
- (5) Coordinating with the G-6/S-6 to develop and maintain user training programs for CIS.
- (6) Identifying to the G-6/S-6 information system support requirements.
- (7) Identifying to the G-6/S-6 specific communications requirements, including requirements to interface with other information systems and potential interface problems.

e. Functional User Responsibilities

On the modern battlefield, it is essential that functional users of information be able to configure and operate the information systems supporting their functional area. Such an ability facilitates increased speed and operator knowledge in establishing a distributed network. It also ensures that functional area users are able to best exploit and control the capabilities of systems that support their needs. Functional users include every staff section that is supported by CIS. Consequently, all staff principals have functional user responsibilities for the functional areas over which they have staff cognizance. For example, the G-3/S-3 has functional user responsibilities for TCO. Functional user responsibilities include—

- (1) Serving as the primary point of contact, both internal and external to the command, for issues affecting information systems supporting the functional area.

- (8) Complying with applicable CIS security measures.
- (9) Reporting malfunctions and outages and coordinating with the G-6/S-6 to restore service.
- (10) Designating an information management officer for the staff section.

f. Communications Between Commands

The responsibility for establishing communications between units must be clearly delineated. These responsibilities are a cornerstone of communications doctrine. However, when supporting combat operations, unit communications capabilities may be destroyed, and responsibility may become unclear or irrelevant. Flexibility, common sense, initiative, cooperation, and mutual assistance must prevail in these instances.

Communications between a senior and subordinate unit are the responsibility of the senior commander.

Communications between adjacent units are the responsibility of the first common senior commander.

Communications between a supporting and supported unit are the responsibility of the supporting unit commander.

Communications between a reinforcing and reinforced unit are the responsibility of the reinforcing unit commander.

Communications between a unit and an attached unit are the responsibility of the commander of the unit to which the attachment is made.

g. G-6/S-6 Staff Cognizance

Communications units and detachments operate under the staff cognizance of the supported unit's G-6/S-6. The Marines assigned to these units, in concert with personnel assigned to G-6/S-6 sections and functional area users, are responsible for employing CIS to support C2. Communications units and the detachments they deploy are the key elements in planning, installing, operating, and maintaining an effective CIS network. See chapter 2 for responsibilities.

Chapter 2

Organizations

Section I

USMC Organizations

Marine Corps CIS are employed to support the command and control of Marine forces. To understand the requirements for CIS support, it is necessary to understand the organization and mission of those forces. Marine forces are organized, trained, and equipped under a total force concept to conduct a wide range of expeditionary operations. The Marine Corps total force consists of three components—the operating forces, the Reserves, and the supporting establishment. The operating forces are an expeditionary “force-in-readiness,” providing forward presence, crisis response, and rapid power projection capabilities to warfighting commanders in chief (CINCs). The Marine Corps Reserve is an integral part of the total force team, is continuously training and operating with the active forces, and is fully prepared to augment or reinforce in times of crisis. The supporting establishment is responsible for recruiting, training, equipping, and sustaining the force—Active and Reserve.

2101. Operating Forces

The two major components of the operating forces are the Marine Corps Forces, Atlantic (MARFORLANT), and Marine Corps Forces, Pacific (MARFORPAC). These two forces constitute the expeditionary combat power of the Marine Corps. The other two elements of the operating forces are the Marine Corps Security Forces at naval installations and the Marine Security Guard Battalion with detachments at embassies and consulates. Consistent with the Goldwater-Nichols Defense Reorganization Act and Joint Pub 0-2, each combatant CINC is assigned a Marine Service component for planning and execution of various

operational plans. MARFORLANT, headquartered in Norfolk, VA, is assigned as the Marine Service component for the U.S. Atlantic Command, the U.S. Southern Command, and the U.S. European Command. MARFORPAC, headquartered at Camp Smith, HI is assigned as the Marine Service component for the U.S. Pacific Command and the CINC United Nations Command/Combined Forces Command.

2102. Marine Corps Forces

Marine Corps forces (MARFOR) is the designation given all Marine component commands. A Marine component command is a command consisting of all MARFOR assigned to a joint force. There are two levels of Marine components. A Marine Service component is assigned to a combatant commander or a subordinate unified commander. (The two standing Marine Service components are described in paragraph 2101.) The other level of component is the Marine component assigned to a JTF. A Marine Service component may consist of one or more MAGTFs, as well as other required theater-level organizations such as a Marine logistic command. Normally, a JTF Marine component will include only one MAGTF and no additional Marine organizations. A MAGTF commander may be dual-designated as the Marine Service or JTF Marine component commander. Unless higher authority establishes otherwise, the Marine component commander commands all assigned MARFOR and exercises operational or tactical control (TACON) of other assigned or attached forces. The Marine component commander deals directly with the joint force commander (JFC) in matters

affecting assigned MARFOR. The Marine component commander commands, trains, equips, and sustains all Marine forces. Combat operations are executed by assigned MAGTFs. When designated by the joint commander, a Marine component commander (at either the Service or JTF level) may also serve as a functional component commander. A functional component command is a command that is normally composed of forces of two or more Military Departments and that may be established to perform particular operational missions. Functional component commanders are normally selected from Service component commanders. Normally the Service component commander providing the preponderance of the functional capability in question is designated the functional component commander. A Service component commander designated as a functional component commander retains Service component responsibilities. A Marine component commander is more likely to be designated a functional component commander in smaller scale contingencies where MARFOR constitute a large portion of the joint force. The Marine component commander could be designated as the joint force maritime component commander, joint force land component commander, or joint force air component commander.

MCWP 0-1.1, *Componency*, describes three possible staff organizations for the component HQ:

- One commander and one staff—A single commander is designated as both the Marine component and MAGTF commander. Likewise a single staff executes both component and MAGTF functions.
- One commander and two staffs—Again a single commander serves as both component and MAGTF commander; however, the commander is supported by two separate staffs.
- Two commanders and two staffs—This organization provides for two separate commanders, each with a dedicated staff. Although this is the most effective arrangement, it is also the most costly in terms of personnel, equipment, and facilities.

2103. Marine Air-Ground Task Forces

Marine operating forces are further organized into MAGTFs. MAGTFs are organized, equipped, and trained to conduct forward-presence and crisis-response missions anywhere in the littoral areas of the world. The MAGTF is capable of conducting expeditionary operations across the full spectrum of conflict, including forcible entry by amphibious assault. The MAGTF is also capable of a broad range of noncombat operations ranging from noncombatant evacuations to disaster relief. Because MAGTFs are task-organized, they differ in organization. However, all MAGTFs share the same basic structure.

a. Core Elements

Each MAGTF has four core elements: a command element (CE), a ground combat element (GCE), an aviation combat element (ACE), and a combat service support element (CSSE). This structure is carefully designed to provide operational flexibility and coordinated execution, thus maximizing the contribution of each element to the overall mission.

(1) CE. The CE is the MAGTF HQ. It is task-organized to provide the command and control capability necessary for effective planning and execution of operations. In addition to the HQ staff, it includes units and detachments that provide communications, information systems, and intelligence support for the MAGTF.

(2) GCE. The GCE is task-organized to conduct ground operations to support the MAGTF mission. It is formed around an infantry organization reinforced with artillery, reconnaissance, armor, engineer, and other forces as needed. The GCE can vary in size and composition from a reinforced infantry battalion to one or more Marine divisions. During amphibious operations, it projects ground combat power ashore by using transport helicopters from the ACE, organic assault amphibious vehicles, and Navy landing craft.

(3) ACE. The ACE is task-organized to perform all or part of the six functions of Marine aviation in support of MAGTF operations. During amphibious operations, it can vary in size and composition, from a reinforced aviation squadron or detachment, with appropriate air command and control and combat service support (CSS), to one or more Marine aircraft wings (MAWs).

(4) CSSE. The CSSE is task-organized to provide the full range of CSS capabilities necessary to support and sustain MAGTF operations. During amphibious operations, it may vary in size and composition from a task-organized CSS detachment to one or more force service support groups (FSSGs).

b. Types of MAGTFs

All MAGTFs are expeditionary forces that are task-organized for a specific mission. MAGTFs vary greatly in size and composition according to the assigned mission. To provide a frame of reference, Marine Corps doctrine categorizes MAGTFs into Marine expeditionary forces (MEFs), Marine expeditionary units (MEUs), and special purpose MAGTFs (SPMAGTF).

(1) MEFs. Most of the Marine Corps operating forces are assigned to the three standing MEFs:

MARFORPAC		MARFORLANT
I MEF	III MEF	II MEF
Based in California	Forward based in Okinawa, mainland Japan, and Hawaii	Based in North and South Carolina

These standing MEFs can deploy as a MEF (normally in echelon) or can deploy subordinate units (task-organized for assigned missions). All three MEFs provide MEUs for service afloat.

The MEF is the principal Marine Corps warfighting organization, particularly for larger crises or contingencies. Normally commanded by a lieutenant general, it is capable of operations across

the full spectrum of conflict, including amphibious assault and sustained combat operations ashore. A MEF can range in size from less than one to multiple divisions and aircraft wings, together with one or more FSSGs. As described above, there are three standing MEFs. Each of these MEFs consists of a permanent CE and one Marine division, MAW, and FSSG. Each forward deploys MEUs on a continuous basis.

The size and composition of a deployed MEF can vary greatly depending on the mission, from elements consisting of less than a full division, wing, or service support group to elements consisting of more than one. A MEF can deploy with forces attached from the other standing MEFs as well as from the Reserves. With accompanying supplies for 60 days, MEFs are capable of both amphibious operations and sustained operations ashore. With appropriate augmentation, especially in the area of C2 capability, the CE is capable of performing the mission of a JTF HQ, and the MEF can serve as the nucleus of the JTF. The CIS requirements associated with such taskings are significant.

A MEF normally deploys in echelon and designates its lead element as the MEF (forward) (MEF [Fwd]). The deployment of the MEF (Fwd) does not automatically trigger the deployment of the entire force. This would occur only if the crisis is large enough to require the entire MEF.

(2) MEUs. The MEU is normally composed of a reinforced infantry battalion, a reinforced helicopter squadron (which may include vertical/short takeoff and landing (V/STOL) attack aircraft), a MEU service support group, and a CE. The MEU is commanded by a colonel and deploys with 15 days' worth of accompanying supplies. MARFORLANT and MARFORPAC routinely forward deploy MEUs aboard amphibious shipping in the Mediterranean Sea, Indian Ocean, Persian Gulf, and Western Pacific. Deployed as part of an amphibious ready group, the MEU provides a combatant or operational commander with a seabased rapid-reaction force for a wide variety of missions. The MEU has a limited forcible entry capability and can facilitate the employment of

follow-on forces, including joint and combined forces as well as a MEF. Before deployment, the MEU undergoes a 6-month training program focusing on selected maritime special operations and culminating in the designation of the unit as “special operations capable” (MEU[SOC]).

(3) SPMAGTFs. A SPMAGTF may be formed to conduct a specific mission that is limited in scope and focus and often in duration. A special purpose MAGTF may be any size, but normally it is a relatively small force—the size of a Marine expeditionary unit or smaller—with narrowly focused capabilities chosen to accomplish a limited mission. Common missions of a special purpose MAGTF include raids, peacekeeping, noncombatant evacuation, disaster relief, and humanitarian assistance.

2104. Marine Corps Forces Reserves

Rapid force expansion is possible through the activation of the Marine Corps Forces Reserve (MARFORRES). The Reserve, like the active forces, consists of a balanced combined-arms team with ground, aviation, and CSS units. Organized under the Commander, Marine Corps Forces Reserve, units are located at 191 training centers in 46 states, Puerto Rico, and the District of Columbia. The Marine Corps Forces Reserve is closely integrated with the active component under the Marine Corps total force concept. The Reserves provide individuals and specific units to augment and reinforce active capabilities.

2105. The Supporting Establishment

The supporting establishment consists of 16 major bases, training activities, formal schools, the

Marine Corps Recruiting Command, the Marine Corps Combat Development Command, the Marine Corps Systems Command, and Headquarters, U.S. Marine Corps. The supporting establishment’s contributions are vital to the overall combat readiness of the Marine Corps. Furthermore, because of the interconnected nature of the CIS support infrastructure, the supporting establishment plays a direct role in supporting the command and control of all MAGTFs. This support is necessary to effectively deploy and implement modern information technology in support of the MAGTF both in garrison and when deployed. In particular, the Marine Corps Network Operations Center and the Marine Corps Tactical Systems Support Activity (MCTSSA) provide essential support to the operating forces in the employment and operation of CIS.

The Marine Corps Network Operations Center, located in Quantico, VA, acts as the focal point for technical support of Marine Corps data communications networks. This activity provides assistance in planning for and maintaining data communications networks for the MAGTF by coordinating with external agencies such as DISA; advising operational planners; providing software support, including contact teams; and providing Marine Corps-wide network operations management.

MCTSSA, located at Camp Pendleton, CA, provides support to the operating forces for the operation and maintenance of fielded CIS. As the designated post-deployment software support activity for most Marine Corps CIS, MCTSSA receives trouble reports, analyzes problems, and takes corrective action. The Fleet Marine Force (FMF) Support Division of MCTSSA provides direct continuous liaison with the operating forces to identify and resolve problems and provides training and operational support for exercises and actual contingencies.

Section II

CIS Organizations

Marines dedicated to using CIS are organized by table of organization (T/O) into the units described in the following subparagraphs. The T/O units may deploy and be employed as a complete unit or they may provide task-organized detachments to support elements of a MAGTF. These units and detachments operate under the staff cognizance of the G-6/S-6 of the supported unit. Separate units and detachments will be found only at higher echelons. At regiments and below, the communications unit will be an integral part of the HQ, and the communications unit commander may also serve as the S-6. The Marines assigned to these units, in concert with personnel assigned to G-6/S-6 sections and functional area users, ensure that an effective CIS network is planned, installed, operated, and maintained. Communications units and the detachments they deploy are the key element in providing CIS capability for the MAGTF elements that they support. Missions, tasks, and concepts of organization and employment of these units are identified in their T/Os and synopsized in this section.

2201. Communication Battalion

The mission of the comm battalion is to provide communications support to a MARFOR component HQ; a MEF CE or a MEF(Fwd) CE; a component HQ deployed simultaneously with a MEF CE and a MEF(Fwd) CE; or two MEF(Fwd) CEs. A further mission is to provide support to three MEU CEs. The battalion provides—

- CE communications for the supported CE: MEU, MEF(Fwd), MEF, and component HQ.
- Communications connectivity between the supported CE and senior, adjacent, and subordinate HQs.
- The supported CE with a Naval Telecommunications Systems entry and/or, as appropriate, entry into the Defense Communications System.

C2 functions are exercised through the battalion commander and the executive staff. The comm battalion consists of the HQ company, a service company, three direct support comm companies, and a general support company. Elements of the comm battalion may be employed separately as task-organized detachments to support organizations smaller than a MEF CE, or the entire battalion may be employed to support larger MAGTF CEs. The HQ company includes the structure necessary to provide detachments to support two MEU CEs.

The comm battalion will normally deploy as a task-organized unit or will deploy task-organized detachments in support of MAGTF CEs. Upon notification, and before deployment of a MEF CE, the battalion will task organize to support the deployment. Upon notification, and before deployment of a MEF(Fwd) CE or a component HQ, a direct support comm company will be task organized to support the deployment. The MAGTF CE G-6/S-6 exercises staff cognizance over MAGTF communications; to facilitate system planning and engineering, the battalion conducts concurrent planning with the Component MAGTF G-6/S-6.

a. HQ Company

The mission of the HQ company is to provide organic command, administration, logistic, and other required support for a comm battalion as well as to support system planning and engineering for and operational control of MAGTF communications networks as required. The company—

- Plans and engineers CIS for the MAGTF CEs, as required.
- Installs, operates, and maintains network control facilities and system control facilities for the component HQ and MAGTF CEs of MEF(Fwd) size and larger.

- Installs, operates, and maintains field message centers, radio links, and tactical switchboard/telephone systems for two MEU CEs.

The company is organized into functional groupings to provide for a battalion and company HQ and support of the primary mission and tasks. The company normally collocates with the battalion HQ and operates in support of the battalion. As required, the various sections can be assigned to task-organized comm battalion detachments in support of deployed MAGTFs.

b. Direct Support Company

The mission of the direct support company is to install, operate, and maintain the communications system for a MEF CE, MEF(Fwd) CE, or component HQ. The company—

- Installs, operates, and maintains communications center facilities for the supported CE/HQ.
- Maintains radio stations on CIS, administrative, logistic, and other radio nets as required.
- Installs, operates, and maintains switchboard and telephone services for the supported CE/HQ.

The direct support comm company is organized into a company HQ and three platoons organized along functional lines, tailored to support the primary mission and tasks listed above. The direct support comm company operates under the direct control of the comm battalion. When operating in support of a MEF CE, the company deploys and collocates with the comm battalion. When in support of a MEF(Fwd) CE or component HQ, the company, with reinforcements, is capable of deploying as a separate unit.

c. General Support Communications Company

The mission of the general support comm company is to install, operate, and maintain the component HQ, MEF CE, and MEF(Fwd) CE message and voice switches and links to JTF HQ, major subordinate commands (MSCs), adjacent units, the Naval Telecommunications System, and the

Defense Communications System as required. The company—

- Installs, operates, and maintains the MEF digital transmission backbone by using cable and multichannel radio (MCR) equipment.
- Installs, operates, and maintains digital switches to provide secure and nonsecure voice, facsimile, message, and data service to the MEF CE CPs.
- Interfaces the component and MEF CE CIS with national systems, the Naval Telecommunications System, commercial telecommunications systems, and senior (CINC/JTF), adjacent, and subordinate systems and networks as required.
- Installs, operates, and maintains tactical wide area networks (WANs)/local area networks (LANs) for MAGTF CEs of MEF(Fwd) size or larger.

The company is organized into a company HQ, a switching platoon, a satellite comm platoon, and a terrestrial comm platoon and operates under the direct control of the comm battalion. When operating in support of the MEF CE, the company deploys and collocates with the comm battalion. When in support of a MEF(Fwd) CE or component HQ, detachments from the company will augment a task-organized direct support comm company to provide a switched communications hub for an area communications network. Simultaneously, ground mobile forces (GMF) satellite communications teams and terrestrial transmission teams, as required, deploy as attachments to MSCs to connect the MEF CE with subordinate commands.

d. Service Company

The mission of the service company is to provide transportation, maintenance, communications-electronics maintenance, materiel handling equipment, materiel handling equipment maintenance, and electrical power distribution services for a comm battalion. The company—

- Provides heavy transportation support to operating companies as required.

- Provides communications-electronics equipment maintenance support to operating companies as required.
- Provides primary electrical power distribution and service for the battalion.
- Provides materiel handling support to the battalion.
- Executes combat trains in support of the battalion.

The service company is organized into a company HQ and three platoons: a motor transport platoon to provide the operation and maintenance of heavy motor transportation equipment organic to the battalion; a communications-electronics maintenance platoon capable of performing third-echelon maintenance on digital switches, telephones, cables, computers, cryptographic equipment, and radio equipment, including high frequency (HF), very high frequency (VHF), ultra high frequency (UHF), super high frequency (SHF), and extremely high frequency (EHF) single and multichannel assets organic to the operating companies of the comm battalion; and an engineer platoon that installs, operates, and maintains power distribution, air conditioning, refrigeration systems, and materiel handling equipment organic to the comm battalion.

When the comm battalion is deployed as a unit, the service company normally collocates with the battalion HQ and provides support. As required, personnel and equipment from the service company can be assigned as part of task-organized comm battalion detachments.

2202. Marine Wing Communication Squadron

The mission of the Marine wing communication squadron (MWCS) is to provide expeditionary communications for the ACE of a MEF, including communications support for the deployment of task-organized elements of a MAW. The squadron—

- Assists in the system planning and engineering of ACE communications and install, operate, and maintain expeditionary communications to support the command and control of the MEF ACE.
- Provides operational systems control centers, as required, to coordinate communications functions internally and externally to the ACE.
- Provides maintenance support for ground-common communications equipment in the MAW.
- Provides the digital backbone communications support for the ACE HQ, forward operating bases, and Marine air command and control system (MACCS) agencies for up to two airfields per detachment. The MACCS agencies include the tactical air command center (TACC), tactical air operations center (TAOC), direct air support center (DASC), early warning/control (EW/C) sites, low altitude air defense (LAAD) teams, and Marine air traffic control detachments (MATCD).
- Provides tactical, automated switching and telephone services for the ACE HQ and TACC.
- Provides electronic message distribution for the ACE HQ, primary MACCS agencies, and tenant units.
- Provides external, single-channel radio (SCR), MCR, and radio retransmission communications support for ACE operations as required.
- Provides deployed WAN and deployed LAN server support for the ACE HQ and primary MACCS agencies.
- Provides the support cryptographic site for all ground-common and MACCS-assigned communications security equipment within the ACE.

The squadron consists of a HQ element and one or two detachments. The squadron provides communications support for the ACE HQ and TACC. Each detachment may be independently deployed to provide external communications for up to two airfields and four forward bases.

2203. Communications Company, HQ Battalion, Marine Division

The mission of the comm company is to install, operate, and maintain the communications system for a Marine division HQ. The company—

- Installs, operates, and maintains communications center facilities for the division HQ.
- Maintains radio stations on CIS, administrative, logistic, and other radio nets as required.
- Installs, operates, and maintains switchboard and telephone services for the division HQ.
- Installs, operates, and maintains MCR terminals for support of internal division communications links as required.
- Provides, in coordination with the artillery regiment, communications support for the division naval gunfire officer, division air officer, and division fire support coordination center (FSCC).
- Installs, operates, and maintains enhanced position location reporting system (EPLRS) master stations and reference community in support of MAGTF operations. The division comm company is organized into a company HQ and six platoons organized by function to support the mission and tasks listed above.

The division comm company will furnish communications for the division main, the division rear, and the alternate CP.

The division comm company will provide multichannel communications to the three infantry regiments, the artillery regiment (which may act as the alternate division CP), and to the DASC. MCR will be the primary means of communication with major subordinate units. Wire communications will not normally be installed to major subordinate units, but may be installed to separate battalions if located within approximately one mile of the division HQ. Otherwise, wire service will be restricted to internal HQ installations for

local telephone and multichannel lines. Multichannel communications service will be disrupted during displacement of the division HQ.

2204. Communications Company, HQ and Service Battalion, FSSG

The mission of the comm company is to provide communications support to the HQs of the FSSG, subordinate battalions, and CSSEs. The company—

- Provides communications support to the FSSG HQ/force CSS area and other CSSEs established to support MAGTF operations.
- Provides communications support for headquarters and service (H&S), maintenance, supply, and dental battalions and augmentation to the organic capabilities of motor transport, engineer support, and medical battalions.
- Installs, operates, and maintains communications control facilities.
- Installs, operates, and maintains tactical automatic switching and wire communications for the FSSG HQ/force CSS area, CSS areas, and, when required, provides small-scale automated switching within maintenance, supply, medical, and dental battalions; the explosive ordnance disposal platoon and bulk fuel company; the engineer support battalion; and the FSSG.

The company is structured to provide communications support to the FSSG HQ in MEF operations and task-organized detachments to the HQs of CSSEs deployed with MAGTFs smaller than a MEF. Augmentation from the MEF comm battalion is required if a dedicated naval telecommunications system/defense communications system entry is required.

The company provides the primary communications support for the FSSG HQ and other CSSE HQs.

2205. Communications Platoons, Branches, and Sections

Comm platoons, branches, and sections provide communications support at the regimental/group, battalion/squadron, and, in some instances, company/battery levels of the MAGTF. These communications units are organized to support the CPs and the communication networks of their parent organization. The artillery unit comm platoons are further required to provide support for establishing the communications links to the units receiving their artillery support. The radio battalion comm platoon provides SI communications support for the MAGTF CE as described further in paragraph 2206. Comm platoons, branches, and sections are found in the following organizations:

a. MEF CE

- H&S company, radio battalion.
- HQ, force reconnaissance company.

b. Marine Division

- HQ company, infantry regiment.
- H&S company, infantry battalion.
- HQ battery, artillery regiment.
- HQ platoon, artillery battery.
- HQ battery, artillery battalion.
- H&S company, tank battalion.
- H&S company, assault amphibian battalion.
- H&S company, combat engineer battalion.
- H&S company, light armored reconnaissance (LAR) battalion.

c. FSSG

- H&S company, engineer support battalion.
- H&S company, landing support battalion.
- H&S company, motor transport battalion.
- H&S company, medical battalion.

d. MAW

- Marine air support squadron (MASS), Marine air control group (MACG).

- H&S battery, LAAD battalion, MACG.
- Marine air control squadron (MACS), MACG.
- Airfield operations division, Marine wing support squadron (MWSS), Marine Wing Support Group (MWSG).

e. MEU

- MEU CE comm platoon.
- H&S company, BLT.
- Comm detachment, MSSG.
- Comm section, MACG, ACE.

2206. Special Security Communications Elements and Teams

The mission of the special security communications elements and teams is to provide SI communications support to the MAGTF. SI communications support for the MAGTF CE is provided by the special security communications element of the radio battalion. SI communications support for the division and MAW HQ is provided by special security communications teams (SS-CT)—small force units organic to each division and MAW. These teams operate under the staff cognizance of the assistant chief of staff (AC/S), G-2/special security officer. The special security element or team provides the personnel and equipment to install, operate, and maintain SI communications terminals. The communications circuits are provided by the communications unit supporting the HQ—the comm battalion for the MAGTF CE, the comm company for the division HQ, and the comm squadron for the MAW HQ. Close coordination is maintained with the supporting SYSCON and TECHCON to ensure adequate support and circuit priority. The special security elements/teams provide personnel augmentation to man ship's signals exploitation spaces (SSES) communications facilities as necessary to support landing force requirements.

2207. Amphibious Squadron Deployment Teams

In 1998, Marine communications detachments (MARCOMDET) and Marine tactical C2 sections (MTACCS) were reorganized into amphibious squadron (PHIBRON) deployment teams to provide support for landing force CIS on board all amphibious ships. As both the Navy and CIS architecture migrates towards a more standardized, digital-based information network, it has become necessary to look at all amphibious platforms as CIS recipients, and couple these CIS requirements with support personnel.

PHIBRON deployment teams provide the required expertise and leadership to maintain Marine Corps current and future CIS networks. The Marine staffing billets as part of the commander amphibious group (COMPHIBGRU) and Fleet staffs will facilitate essential amphibious CIS planning, coordination, installation, and maintenance. In addition, the PHIBRON deployment teams provide appropriate manpower to address critical deficiencies in amphibious CIS requirements determination and programming at Flag and staff levels, as well as necessary operational support.

Section III

C2 Organizations

To exercise command and control in combat, all MAGTF units establish CPs, which serve as the HQ from which the commander and his staff operate. Units of battalion size or larger may divide the HQ into echelons—main, rear, and tactical. The CP then becomes the echelon at which the commander is physically located. The main echelon (main) is where the commander is normally located with those elements of the staff required to plan and direct operations and control forces. In a large geographic area, a unit may establish a rear echelon (rear) to serve principally as an administrative and logistical support base. To be in close proximity to subordinate units and more directly influence tactical actions, the commander may create a tactical echelon (tactical CP). The tactical echelon is mobile and contains a minimum number of personnel and equipment, including the commander, CIS operator(s), the G-2/S-2, the G-3/S-3, and the fire support coordinator.

2301. MEF CE

The MEF staff and supporting CE units are task organized to exercise command and control and to support the MEF's assigned mission. The MEF includes standard components as well as components that are used only for certain missions. Standard components include the principal staff sections and, within the operations section, a future operations cell and a current operations cell. Additional components may be added, based on the mission, to support functions needed in a particular operation. For example, in a humanitarian operation, the MEF commander may organize an agency or section to coordinate with other government (foreign or domestic), nongovernment, and private voluntary agencies and organizations. Another example, establish a consolidated military engineering group to provide centralized planning and manage engineering assets of the Marine Corps, Army, and Navy that are assigned to the MEF.

a. Future Plans

The MEF G-5 establishes a future plans cell to conduct long-range planning. Future plans works closely with the JTF HQ to ensure that the MEF is prepared for its next major mission. Products from future plans provide the basis on which future operations will develop the operations order (OPORD).

b. Future Operations

The MEF G-3 establishes a future operations cell that is responsible for planning operations in support of the current mission. Future operations receives an initial plan and related material from future plans and begins detailed planning. Future operations consists of several full-time personnel from the G-3 who form the core of an operational planning team. When the operational planning team is formed, it includes members of the G-1, G-2, G-4, G-5, and G-6 sections. Other appropriate staff sections join the planning team as needed. Representatives from subordinate units also join the team. Designated functional experts complete this group. The operational planning team remains together through mission analysis and COA development, analysis, and comparison/decision. These personnel then return to their respective work sections, complete annexes and appendices to the OPORD as required, and resume normal duties.

c. Current Operations

The MEF G-3 establishes a current operations cell that is responsible for executing operations. Current operations personnel receive the plan from future operations and execute it. Current operations personnel man the MEF combat operations center (COC) from which they monitor MEF operations and respond to situations as needed. The COC consists of a G-3 watch officer, a G-2 watch officer, a senior watch officer, and a situation report watch officer. A number of enlisted Marines assist in operating tactical information systems

and maintaining situation displays. The G-2 and G-3 watch officers receive information from collocated MAGTF all-source fusion center (MAFC) personnel and force fires coordination center (FFCC) representatives (ground and air), the surveillance and reconnaissance center (SARC), as well as subordinate and adjacent units. The G-2 and G-3 watch officers filter this information and forward important pieces to the senior watch officer. The senior watch officer also receives information that affects current operations from other principal staff sections (G-1, G-4, and G-6). The senior watch officer evaluates information in the context of current operations and determines whether action is required. Depending on the situation, the senior watch officer may be assisted in this process by other officers from current operations. On the basis of authority delegated by the MEF commander, the senior watch officer acts by either issuing orders or briefing the MEF commander and recommending action.

d. C2 Facilities

Watch officers and supporting personnel from the staff sections and supporting units establish and operate centers within the HQ from which the day-to-day activities of the MEF are coordinated, controlled, and supported. These C2 centers sometimes, especially when dealing with air command and control, are referred to as C2 agencies. In this publication, these centers and agencies, both at the MEF level and at the subordinate unit level, are referred to as C2 facilities. These facilities include the personnel, software, hardware, shelters, and ancillary equipment needed to support command and control. The key C2 facility in the MEF is the COC described above. In most cases, the COC is collocated with the FFCC and the MAFC. These three C2 facilities work together closely, focusing on current operations and responding to the immediate needs of the MEF commander. In all cases, information system support and LAN connectivity within and among these three facilities are essential for efficient execution of MEF operations. The FFCC, the MAFC, and other MEF C2 facilities are discussed under the functional area they support.

e. MEF Rear

The MEF rear may perform several functions within the MEF area of operations (AO). A MEF rear may be established to coordinate administrative and logistical activities while the MEF maneuvers forward. The MEF rear may also be assigned responsibility for rear area operations. Rear area operations are extremely complex at the MEF level. Joint doctrine currently defines eight rear area functions that must be coordinated: area management, movements, infrastructure development, host nation support, security, communications, intelligence, and sustainment. The MEF commander may assign some or all of these functions to the MEF rear and others to the wing and the FSSG. If assigned overall responsibility, the MEF rear would require the capability to plan and conduct rear area operations. In this instance, the MEF rear would establish a rear area operations center to facilitate command and control of operations within the rear area. In situations where the main HQ does not move forward and the MEF retains responsibility for rear area operations, the rear area operations center becomes another element of the MEF.

2302. Ground Combat Element

a. Division Main

The division main serves as the division commander's primary HQ. Both current and future operations planning are accomplished in the division main. Division personnel monitor current operations from the division main, and if the commander is aboard, current operations are also directed from the division main. Although smaller than the MEF, the division main is organized for command and control in a similar manner, including a future operations cell within the G-3 section. Current operations are directed from the division COC, which is typically manned with G-3 personnel; G-2 personnel; the division engineer; the division air officer; and nuclear, biological, and chemical (NBC) personnel. The FSCC is usually physically collocated with the COC, and the DASC is either physically or electronically collocated with the FSCC.

b. Division Rear

If the division is spread over a large geographic area, the division commander may establish a division rear. The division rear may serve principally as an administrative and logistical support base for the division. In this arrangement, the division main may consist of the COC and FSCC with the collocated DASC. The division rear would then include principal staff elements not required to plan and execute current operations (G-1, G-4, staff judge advocate, etc.). This arrangement allows the division main to maneuver rapidly in high-tempo operations.

c. Division Tactical Echelon

The division commander may establish a small, highly mobile tactical echelon to remain in close proximity to the battle, gain first-hand situational awareness, and more directly influence tactical operations at critical times. Depending on the situation, either surface or air platforms, appropriately configured, provide mobility and communications for the tactical echelon. The division commander prescribes which staff members constitute the tactical echelon. A nominal tactical echelon would include the division commander, CIS operator(s), G-2, G-3, and fire support coordinator.

d. Regiment/Battalion

Regiments and battalions also use the main, rear, and tactical echelon structure and establish a COC to coordinate and direct operations. These operations centers and echelons are much smaller than those at the division level because regiments and battalions have fewer subordinate units and fewer functions to support.

e. Tactical Air Control Party

Tactical air control parties (TACPs) provide coordination between GCE units and supporting aviation assets. TACPs exist at the infantry division, regiment, and battalion levels. Depending on the command level, a TACP contains a combination of air officers, forward air controllers, and enlisted radio operators. Air officers serve at the division, regiment, and battalion levels. These officers serve as special staff officers to their re-

spective commanders. Additionally, they may serve within the FSCC to assist with planning and deconfliction functions related to air support for the assigned unit. Forward air controllers provide terminal control of close air support aircraft that are passed to them by the DASC. These officers also advise GCE commanders on aviation capabilities and limitations and prepare requests for air support.

2303. Aviation Combat Element

a. Wing Main

The wing main serves as the principal HQ for the wing commander. Like the MEF and division main, most principal staff members are located in the wing main, and future planning is done in the wing main. The wing rear area operations center is often collocated with the wing main. Unlike the MEF and division main, however, the wing main may be located outside the MEF AO. The wing commander often locates the wing main at a large airfield, especially if this airfield houses most of the wing's fixed-wing aircraft. Wing future and current operations functions occur within the TACC, which may or may not be collocated with the wing main.

b. TACC

The wing commander conducts future operations planning and current operations monitoring from the TACC. The TACC consists of three mutually supporting cross-function operational cells supported by a centralized intelligence center. The organizations that comprise the TACC are—

- Future plans
- Future operations (future ops)
- Current operations (current ops)
- Air combat intelligence (ACI)

Future plans conducts aviation and aviation support planning for the next MAGTF mission change. Future ops develops future air tasking orders (ATOs), and prepares OPORDs/fragmentary orders for the next ACE mission change. Current

ops executes the daily ATO and assesses its effectiveness.

ACI is imbedded within the TACC. Timely, tailored, and fused intelligence is integral to the functioning of future plans, future ops, and current ops. ACI is the focus of all aviation intelligence activities supporting the ACE. It produces and disseminates aviation specific all-source intelligence, including assessments of adversary capabilities and vulnerabilities, target analysis, battle damage assessment (BDA), and the current status and priority of assigned targets to assist in execution day changes. The TACC uses specialized information systems and equipment to display a common picture of the aviation situation received from tactical digital information links. Each Marine aviation function (antiair warfare, assault support, electronic warfare (EW), air reconnaissance, offensive air support, and control of aircraft and missiles) provides representation to the TACC.

c. TAOC

The TAOC performs air surveillance and control of aircraft and missiles for the wing commander. Air control personnel assigned to this facility use specialized information systems, sensors, and dedicated communications links to search the MEF's airspace and provide air defense services for those areas designated as vital. The TAOC controls friendly aircraft in the intercept of hostile aircraft and assists Marine missile units in locating and destroying hostile aircraft. Information gained through radar assets and tactical digital information links is transmitted to the TACC and provides situational awareness for the wing commander. The TAOC is movable, but not mobile, and is located in the rear of the MEF AO. Often, the TAOC is collocated at a fixed-wing airfield.

d. MATCDs

MATCDs provide air control services in and around airfields. Additionally, detachment radar contributes to air surveillance efforts, and information is forwarded to other agencies via tactical digital information links. Detachment personnel

coordinate with Stinger teams to construct and operate base defense zones.

e. LAAD Battery Command Center

The LAAD battalion, usually collocated with the TAOC, establishes a COC for the exercise of battalion operations. The LAAD battalion commander exercises overall command and control of LAAD battalion operations from the COC. The LAAD battalion commander obtains and relays intelligence and combat information on friendly and enemy operations to the two subordinate LAAD battery COCs. The LAAD battery COCs maintain situational awareness of MAGTF and other air operations and plan and control employment of LAAD teams.

f. DASC

The DASC controls aircraft supporting the GCE. Air support personnel control aircraft en route to the forward air controllers serving with infantry units. DASC controllers also monitor helicopter missions within the MEF battlespace. These personnel assist GCE units to obtain additional air support, either fixed-wing aircraft or helicopters, beyond those preplanned missions scheduled to fly. Because of their proximity to the senior FSCC, DASC personnel often help the wing commander maintain awareness of the ground combat situation. Several configurations exist for the DASC, with varying degrees of size, capability, and mobility. One configuration may be employed in a C-130 aircraft.

g. Airborne Coordinators

Marine pilots and aircrew often serve as airborne extensions of MACCS. The tactical air coordinator (airborne) serves as an extension of the DASC and coordinates aircraft en route to close air support missions. The tactical air coordinator (airborne) receives aircraft "hand-offs" from the DASC, briefs those aircrew, then turns these missions over to ground or airborne forward air controllers for terminal control. The assault support coordinator (airborne) also serves as an extension of the DASC and coordinates complex helicopter missions. The assault support coordinator decon-

flicts transport packages, escort packages, and fire support efforts throughout the mission.

Airborne strike coordination and reconnaissance is a means to efficiently focus aviation fires in the deep battlespace. This function, usually performed by an F/A-18 aircrew, allows real-time reconnaissance to locate the MEF commander's high-priority targets. Once located, the strike coordination and reconnaissance aircrew control attack aircraft in much the same manner as a tactical air coordinator, cycling and deconflicting multiple strike packages as they ingress to the target area. Using aircrew to extend the command and control system offers several benefits. These personnel can position themselves to effectively control multiple aircraft missions and maintain communications with both the aircraft they control and ground-based C2 facilities.

2304. CSSE

a. FSSG Main

The FSSG main is task organized by the FSSG commander to enable him to control and coordinate logistic support of the MEF. An FSSG main includes the principal staff sections, a future plans and deployment section, and the CSS operations center (CSSOC). The future plans and deployment section ensures that the FSSG is prepared to support the next major mission of the MEF. Often, this new mission involves a deployment or redeployment. The CSSOC monitors current operations and plans near-term future operations. The FSSG main will typically be located near sea or aerial ports of debarkation in the MEF's AO. Subordinate battalions establish their own HQ in proximity to the FSSG main.

b. CSSOC

The CSSOC serves as the hub for future and current operations planning within the FSSG main. Each CSS functional area (supply, maintenance, transportation, engineering, health services, and services) provides representation to the CSSOC. Under the supervision of a G-3 watch officer, these personnel monitor current operations and

maintain status displays of friendly and enemy situations. Additionally, CSSOC personnel handle requests from subordinate units and keep the MEF informed of the CSS situation. FSSG commanders may choose either a centralized or decentralized configuration for their CSSOCs.

c. Combat Service Support Detachments

Depending on the situation, the FSSG commander establishes forward detachments to provide direct support to the GCE. Detachment commanders may establish small facilities to coordinate support and monitor logistics communications nets. A mobile CSS detachment possesses the least capability to establish an operations center. In this instance, the CSSOC could resemble a mobile, tactical echelon. Communications connectivity would be predominantly through SCR.

d. Movement Control Center

Movement control centers support the deployment of the MEF from the home station, through intermediate bases, to the destination. The commander, MARFOR (COMMARFOR) establishes a HQ movement control center, which provides connectivity to United States Transportation Command (USTRANSCOM) and keeps the MEF force movement control center apprised of strategic movement issues. The force movement control center controls and coordinates all movement support and conducts liaison with the Air Mobility Command, the Military Sealift Command, and the Military Traffic Management Command. The force movement control center supervises efforts of unit movement control centers of the division, wing, and FSSG. These latter units provide transportation and communication assets in support of deployment activities. Bases and air stations from which Marine units deploy establish base or station operations support groups to coordinate their efforts with those of deploying units. These bases also provide their transportation and communication assets in support of deploying units. These units augment unit movement control centers to ensure that all personnel and materiel arrive at sea and aerial ports of embarkation.

e. Marine Logistic Command

The COMMARFOR may establish a Marine Logistic Command (MLC) and assign it responsibility for establishing the theater general support structure to facilitate reception (arrival/assembly) and reception, staging, onward movement, and integration operations, and, on order, for providing operational logistic support to Marine forces as the Marine component operational-level logistic agency in theater. MLC is a task organization option, not a standing organization. COMMARFOR may choose to assign a specific FSSG responsibility for MLC functions. Then, on the basis of the operational situation, theater geography, operations and logistic command and control, and infrastructure requirements, COMMARFOR will assign Marine component resources to the FSSG for detailed task organizing and conducting MLC theater-support operations.

2305. Intelligence Command and Control

The combat intelligence center (CIC) is established under the G-2/S-2 within the MAGTF HQ to provide centralized direction for the overall MAGTF intelligence effort. This organization serves the entire force by consolidating, validating, and prioritizing intelligence requirements from all MAGTF elements. The CIC links the MAGTF to JTF, theater, national, and allied intelligence assets. The CIC includes as key internal nodes the MAFC and the SARC. It also provides small G-2/S-2 elements to support both the current and future ops cells. The CIC is supported by the reconnaissance operations center and the operations control and analysis center (OCAC).

a. MAFC

The MAFC provides intelligence analysis, production, and targeting information to the MEF. An integral part of the MAGTF main CP, the MAFC is usually collocated with the MEF COC. All surveillance, reconnaissance, and intelligence gathering results flow into the MAFC, where they are fused with previous collections and intelligence products are updated and disseminated.

b. SARC

The SARC is the primary intelligence C2 node used to direct, coordinate, monitor, and supervise MAGTF collection operations (including intelligence collection operations conducted by organic attached and direct support assets). The SARC is located close to the MEF COC. The SARC coordinates collection and operations tasks to various MEF assets, including force reconnaissance, the sensor control and management platoon, the unmanned aerial vehicle squadron, the radio battalion, counterintelligence detachments, interrogator-translator teams, the force imagery interpretation unit, and the topographic platoon. Collection results are forwarded to the MAFC to incorporate into current intelligence products, and, when appropriate, to the COC.

c. Reconnaissance Operations Center

The reconnaissance operations center serves as a focal point for monitoring and supervising force reconnaissance operations. Located near the SARC, this facility gathers information from dispersed teams, decrypts reports, and forwards information for fusion into the overall MEF intelligence situation display. Personnel manning the reconnaissance operations center assist reconnaissance teams with movement and other activities as needed.

d. OCAC

The OCAC provides centralized direction, management, and control of signals intelligence (SIGINT) and EW activities within the MEF and coordinates with external theater and national assets. Assigned personnel process, analyze, and disseminate collected information. The OCAC is located within the MEF HQ compound, near other intelligence C2 facilities.

e. Intelligence Centers

The G-2/S-2 will establish intelligence centers at all echelons of the MAGTF down to the battalion level. Personnel assigned to the intelligence center will collect, process, integrate, analyze, evaluate, and interpret intelligence and continuously update the enemy situation. This information will be rapidly provided to current and future ops.

These centers will be collocated with the COC whenever possible.

2306. Fire Support Centers

C2 facilities are established to coordinate the overall fire support effort and to exercise tactical and technical fire support direction.

a. FFCC

The FFCC is established at the MEF level to assist the MEF commander in planning and coordinating deep fires. The FFCC performs three primary functions for the MEF: planning, acquiring, and maintaining target information; coordinating and integrating MAGTF-level fires with future operations; and coordinating and integrating MAGTF-level fires into current ops. Located within the MEF, this facility assists both future ops and current ops in their targeting functions. Additionally, the FFCC provides coordination between the MEF and JTF targeting boards and centers. Watch standers may be collocated with the COC to facilitate rapid deep fires coordination.

b. FSCC

Each Marine ground combat organization from division to battalion employs a FSCC as an advisory and coordination agency. The FSCC is collocated with the COC. The senior FSCC coordinates and deconflicts fire support efforts among subordinate units and centers. The FSCC includes the fire support coordinator, artillery liaison, TACP personnel, mortar unit liaison when appropriate, and a naval surface fires liaison. At the division level, the division artillery officer or artillery regiment commanding officer serves as the fire support coordinator. At lower levels, each commander appoints a fire support coordinator from his staff (usually the weapons company commander).

c. Fire Direction Center

Fire direction centers (FDCs) exist at artillery regiments, battalions, and batteries. These organizations permit respective commanders to plan and control fires. Fire direction activities may be centralized or decentralized. At regimental and bat-

talion levels, the FDC exercises tactical fire direction, and battalion FDC personnel supervise, advise, and augment battery personnel as required. Battalion personnel also assist by troubleshooting gunnery problems, which enables battery FDC personnel to focus on delivering artillery fires. The battery FDC provides technical fire direction by evaluating information received by forward observers and determining firing data. This firing data is issued to artillery sections through fire commands. Battery FDCs are also capable of tactical fire direction and would perform this function in cases, such as MEU deployments, when the battery operates independently.

d. EW Coordination Center

The EW coordination center (EWCC) facilitates coordination of EW operations with other fires and CIS. This center coordinates efforts by the G-2, G-3, and G-6 to eliminate conflicts between these overlapping battlespace functions. The EWCC is under the staff G-3's cognizance. Assigned personnel identify potential conflicts in planned operations and work to resolve these issues. The EWCC includes an EW officer, a CIS representative, and other liaison officers as needed. Liaison could include radio battalion representation, EA-6B electronic countermeasures officers, a MACG radar officer, and other Service representatives.

2307. Rear Area Operations Centers

Responsibility for rear area operations may be tasked to the MEF rear. It may also be shared with or assigned to the FSSG and the wing, especially when the MSCs are widely dispersed geographically. In any case, a rear area operations center facilitates C2 operations within the rear area(s). The rear area operations center contains personnel to monitor and coordinate the vast array of activities occurring in the MEF rear area. For MSCs, the size and scope of a rear area operations center would be driven by the unit's mission and rear area activities. At a minimum, the wing and FSSG would use one or more rear area operations centers to coordinate security for the bases they occupy. Personnel serving in these facilities must be

knowledgeable in all functions performed by the facility. To support the security function, a fire support coordinator must be assigned to plan and coordinate fires in the rear area. All rear area operations centers should be linked and should coordinate activities across the entire MEF rear area.

2308. CIS Control

At the MAGTF CE level, the CISO (G-6/S-6) exercises overall operational systems control of MAGTF communications networks and information systems. The G-6/S-6 also coordinates with the controlling authorities of external networks. The G-6/S-6 is assisted by personnel from the communications battalion to exercise operational systems control. Operational systems control is exercised at levels lower than the MAGTF down to the battalion/squadron level by the G-6/S-6 of that organization. The G-6/S-6 is supported by organic communications units or detachments.

a. Operational Systems Control Center

The functions of an operational systems control center (OSCC) exist at all levels of CIS control. At higher echelons (MSC and above), specific agencies are established to conduct these functions. At lower echelons (bn/sqdn), the functions are still performed, but at the S-6/comm unit level. Figure 2-1 details a typical Joint operational systems control model. The OSCC functions consist of the following:

(1) Systems Planning and Engineering. The systems planning and engineering (SPE) performs future ops functions for communications operations. The SPE at any echelon consists of CIS network design. These networks are designed and subsequently engineered to meet the operational requirements as determined by the CISO. Circuits are determined by type and number to meet both internal and external command communications requirements. SPE personnel normally perform their duties in a suitable facility as part of the G-6/S-6 staff in the main CP. The MAGTF G-6/S-6 is the senior Marine CISO who directs the overall

SPE effort at the MAGTF level. The G-6/S-6 at lower echelons, with the assistance of their supporting communications unit/detachment, performs appropriate level SPE functions in accordance with the overall MAGTF communications plan.

(2) Systems Control. The systems control (SYSCON) performs current operations functions for communications operations. The SYSCON is established by the operations officer of each communications unit to maintain current information on availability and operational readiness of CIS, set priorities and resolve conflicts. SYSCON personnel perform their duties in an appropriate facility in the vicinity of the supported command post. The SYSCON receives direction from the SPE. The SYSCON coordinates directly with senior, subordinate, and adjacent SYSCONs as required. SYSCON personnel must have the technical expertise and experience to coordinate resolution of complex communications problems.

(3) Technical Control. TECHCON provides centralized technical supervision over the installation, operation and maintenance of single channel radio, wire, multichannel and data communications systems. TECHCON functions are performed from specially designed TECHCON facility(ies), the network operations center, maintenance facilities, and communications centers, when established. The TECHCON facility(ies) provides a means to conduct and coordinate circuit troubleshooting and restoration. The size and scope of the TECHCON facility(ies) are driven by the size of the communications organization and types of services being provided. TECHCON personnel must have the technical expertise and experience to resolve complex communications problems.

b. Joint Communications Control Center

The joint communications control center (JCCC) is the operational systems control agency of the JTF or CINC J-6. Per Chairman, Joint Chiefs of

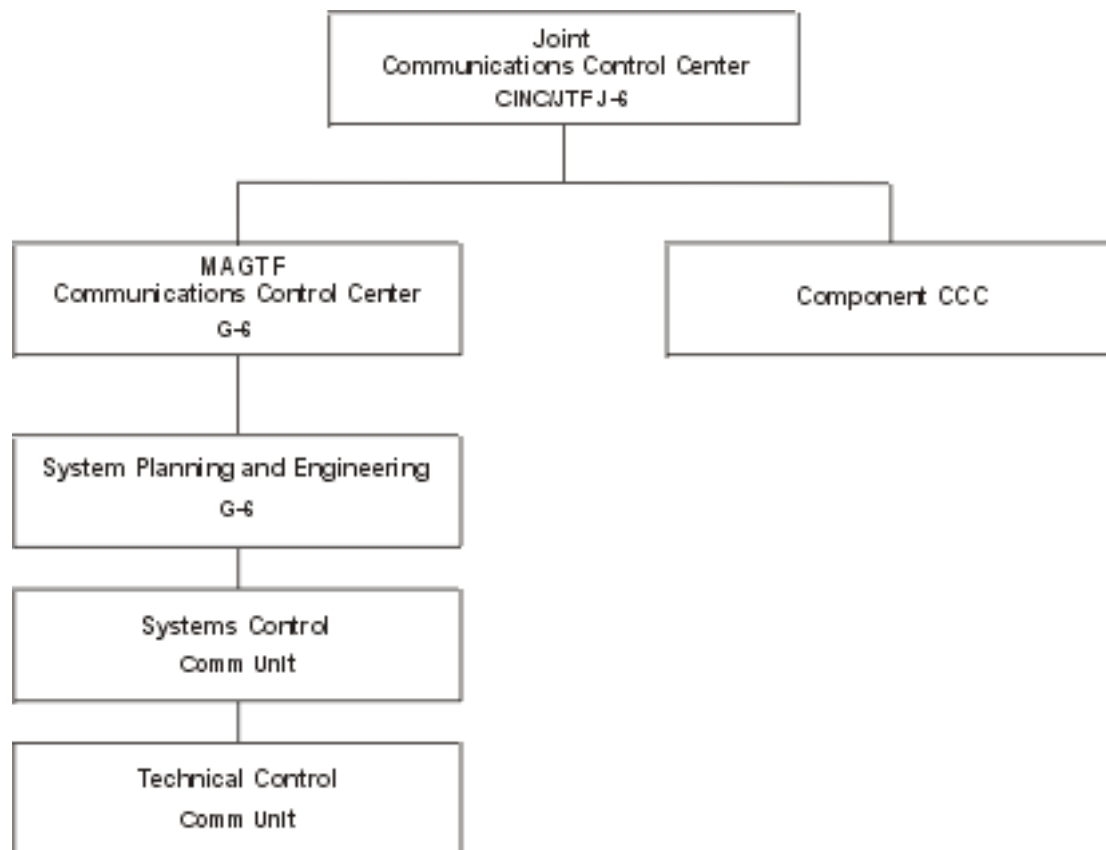


Figure 2-1. Joint Operational Systems Control Model.

Staff Manual (CJCSM) 6231.07A, *Joint Network Management and Control*, the JCCC provides theater or JTF planning level and supervision of component communications control centers. Normally, liaison officers from each service component command are provided to the JCCC as subject matter experts and participate in JCCC functions as watch members.

c. MAGTF Communications Control Center

The MAGTF G-6 employs the MAGTF communications control center as the MAGTF operational systems control center. The subordinate communications battalion(s)/company(ies) staff augments the MAGTF communications control center. The MAGTF communications control center coordinates external communications control with the JTF or CINC J-6 through the JCCC. The

MAGTF communications control center may also be required to support to a Marine component HQ.

d. Component Communications Control Centers

Each component of the Joint Force or Theater Command (USA, USAF, USN, USMC) establish some form of an operational systems control center to perform component level operational systems control functions. The components of the designated army Theater Signal Command will normally support the Army Component Command and augment JTF/Theater-level operational systems control agency. The MAGTF communications control center will coordinate OSCC functions with joint and service component communications control centers to maintain the joint network.

2309. Amphibious C2 Facilities

When the MAGTF is embarked aboard amphibious shipping, the MAGTF commander serves concurrently as the commander of the landing force. While embarked, the MAGTF commander and his staff direct the actions of the MAGTF from C2 facilities aboard the amphibious ships. Under the OMFTS concept, MAGTF command and control may remain afloat throughout the amphibious operation. Many of the shipboard C2 facilities also support the commander, amphibious task force (CATF), who normally is located, with his staff, in the flag plot located aboard the flagship.

a. Landing Force Operations Center

The landing force operations center (LFOC) is the shipboard space allocated to the commander, landing force (CLF), and staff to plan and execute landing force operations. The LFOC is normally located on the amphibious task force (ATF) flagship. The LFOC staff are the same personnel who man the MAGTF COC when and if it is phased ashore in an amphibious operation. The functions of the LFOC mirror those of the COC. This center controls and monitors the activities of the landing force until the CLF establishes command ashore.

b. Amphibious Task Force Intelligence Center

The amphibious task force intelligence center (ATFIC) is a single Naval intelligence facility formed during a preassault phase of amphibious operations. It supports the requirements of the CATF and the CLF. The ATFIC is usually located aboard the amphibious flagship and is manned by Navy and Marine intelligence personnel. Intelligence resources available to the ATFIC include national, joint, combined, and internal naval force assets. Some of these assets may already be forward deployed in advance or assault operations. Landing force intelligence personnel and their organic information systems such as the Intelligence Analysis System (IAS) and the technical control and analysis center (TCAC) workstations are integrated in the ATFIC operations while afloat. Additionally, the ship's signals exploitation space (SSES) is within the ATFIC and con-

tains ATF special security communications terminals and processing facilities.

c. Supporting Arms Coordination Center

The CATF exercises overall coordination of supporting fires within the amphibious objective area through the supporting arms coordination center (SACC). This center, located aboard the amphibious flagship, consists of a supporting arms coordinator, naval gunfire, air support, and target information sections. ATF operations, intelligence and communications personnel, and landing force fire support personnel perform the functions of the SACC. These functions are similar to those performed by the FFCC and FSCC that may be subsequently established ashore. A landing force liaison is established in the SACC if the responsibility for coordination of supporting arms is passed ashore.

SACC provides the commanders of the ATF and the landing force with information concerning the requirements and developments that affect coordination of fire delivery by naval gunfire units, support aircraft, and artillery units. Fire support requests received from the landing force are coordinated from this center to ensure that all fires are integrated to achieve the maximum effect against targets. Current fire support information is continually updated and displayed while direction for the execution of restrictive fire plans and instructions concerning troop safety are promulgated. Naval gunfire plans are prepared and their execution is supervised by the SACC staff. This center also coordinates air support operations with appropriate ATF and landing force air control agencies. Records of targets in the objective area are maintained, and appropriate fire support activities in the amphibious objective area are monitored when responsibility for the coordination of fires is passed to the CLF ashore.

d. Tactical Air Control Center (Afloat)

The tactical air control center (afloat) (TACC[A]) is organized and located in the flagship of the CATF. The TACC(A) provides the means to direct and coordinate all tactical air operations in an objective area, including antiair warfare, until this

responsibility is transferred to Marine air control agencies ashore. The TACC(A) consists of a tactical air controller; air support controller; antiair warfare coordinator; and appropriate operations, intelligence, and communications personnel and equipment. These personnel and their equipment are provided by the flagship, the staff of the CATF, and a designated tactical air control squadron.

e. Helicopter Direction Center

The helicopter direction center (HDC) is organized aboard the flagship of the helicopter transport group to provide the means to direct and control helicopters during the ship-to-shore movement. It consists of a helicopter director, who is responsible to the tactical air commander for direction of all helicopters and supporting aircraft; a helicopter direction net officer; a helicopter air controller; and other appropriate air operations and communications personnel and equipment. These personnel and their equipment are normally provided by the flagship on which the HDC is established.

To effect the direction and control of helicopter movement in an objective area, the HDC must operate under the overall direction of the TACC(A) for coordinating air operations with other agencies and under the operational control (OPCON) of the helicopter transport group commander. The HDC advises the TACC(A) on all matters pertaining to helicopter movement that require coordination with supporting arms. The HDC provides information as directed by the TACC(A) and the helicopter transport group commander and maintains availability and location status of assigned helicopters. The HDC also receives requests for helicopter support, designates units to provide the helicopters for specific missions, and directs their employment. The HDC further controls the movement of helicopters, both transport and escort, from wave rendezvous to initial point and from takeoff at the landing zone to breakup point. The HDC also controls movement of helicopters between platforms and assists the DASC in controlling helicopters between ship and shore after the control of helicopters has been passed ashore.

f. Tactical-Logistical Group

Tactical-logistical groups (TACLOGs) are temporary agencies organized as required by ground combat organizations of a landing force to assist the naval control organization in the ship-to-shore movement of troops, equipment, and supplies. They are normally established aboard control ships at each echelon of the MAGTF, along with the naval control agency exercising control over the ship-to-shore movement of that echelon during a waterborne landing. They are also established aboard each helicopter transport carrier during vertical assaults. A TACLOG consists of operations, CSS, embarkation, and communications personnel provided by the parent ground combat organization.

TACLOG assists the corresponding naval control agency in handling landing force requirements during the ship-to-shore movement. It is task-organized to advise the naval control agency as to the location of units, equipment, and supplies and to monitor their regulated movement ashore. The TACLOG maintains a detailed record of the unloading and landing status, provides information to appropriate commanders concerning the progress of the ship-to-shore movement, and responds to routine requests received from units by coordinating with the naval control agency. It further advises the naval control agency when the tactical situation ashore dictates an adjustment to the prescribed landing sequence.

2310. Mobile CPs

Mobile CPs provide means for commanders at all levels to keep pace with rapidly maneuvering elements. They are essential for the conducting maneuver warfare. These mobile CPs are usually mounted in vehicles, but may be situationally airborne or footmobile. Various configurations exist depending on the availability of C2 platforms. C2 variants of the assault amphibious vehicle (AAV) and light armored vehicle (LAV) are specifically designed for this purpose, and it is also one of the roles of the utility helicopter. Units also use organic vehicles in various arrangements to form mobile CPs. Mobile CPs normally consist of the

commander accompanied by a few key personnel from the tactical echelon. At the small unit level (rifle company and rifle platoon), the CP is often footmobile. In some situations, the tactical echelon of a larger unit may be footmobile; for exam-

ple, when operating in terrain that precludes using vehicles. However, given restrictions on the amount of equipment that can be carried, a footmobile CP is usually impractical above battalion level.

Chapter 3

Information Systems and Services

Information systems and services provide the management and decision support tools that are required to support command and control functions, including operations planning and execution. To improve interoperability, increase efficiency, and reduce costs, the DOD has mandated that the Services move to a common set of information systems and services. This migration is taking place rapidly with the fielding of the GCCS and the implementation of the defense information infrastructure (DII) common operating environment (COE). These developments are having a

profound effect on Marine Corps CIS policy and will ultimately have an impact on all MAGTF CIS doctrine, organization, training, and equipment. The Marine Corps is migrating its tactical information systems to the DII COE beginning with TCO and IAS. DII COE compliance will provide complete interoperability with GCCS and other DII COE-compliant systems. To understand the information systems and services provided by the MAGTF CIS environment, it is necessary to describe that environment in the context of the GCCS and the DII COE.

Section I

Defense Information Infrastructure Common Operating Environment

The DII COE provides a standard environment, off-the-shelf software, and a set of programming standards that describe in detail how mission applications will operate in the standard environment. The COE contains common support applications and platform services required by mission applications.

3101. Mission Applications

Each mission application that is migrated to the common environment must comply with guidance published in the DII COE standards (see app. A). Although there may be some need for “workarounds” as mission applications migrate to the COE, these are necessary as mission applications. As the COE matures, workarounds will no longer be needed and will be stripped from the mission application.

3102. Services

As the user selects the mission applications needed to perform a set of tasks, the integration tool automatically loads all the COE modules needed by those applications. These selected modules make up a subset of the DII COE superset: this subset is called a COE-variant (COE-V). The original COE software components are used without modification. System managers must ensure that COE-Vs do not include nonstandard software that duplicates services provided by software under the COE. Figure 3-1 (on page 3-2) shows the services available under the DII COE. This figure depicts mission applications (e.g., Joint Maritime Command Information System [JMCIS]) accessing the services in the DII COE through a standard application interface. It also reflects both the mission applications and the DII COE services hosted on common computer platforms using COTS operating systems.

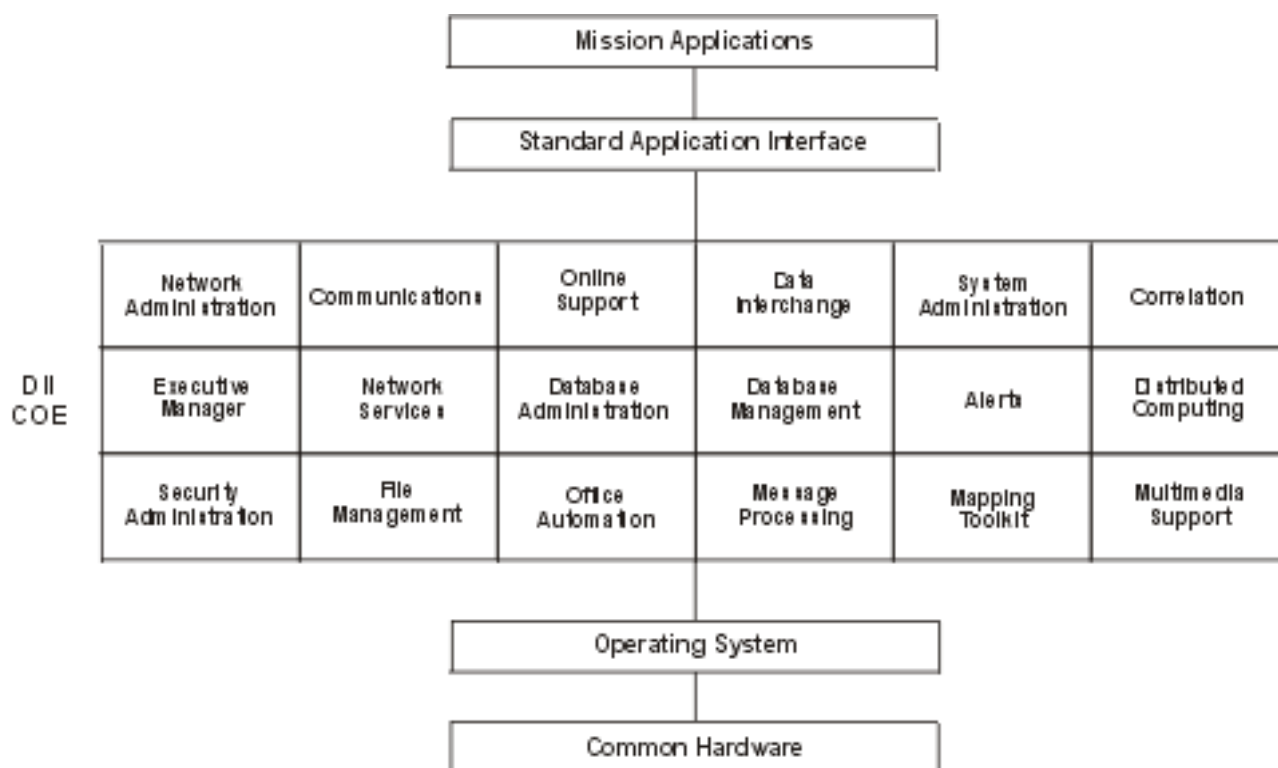


Figure 3-1. D II COE Services.

Section II

Global Command and Control System

The GCCS implements the joint C4I for the warrior concept. This concept calls for the capability to move a joint force anywhere on the globe at any time and to provide that force with the information necessary to accomplish its mission. The GCCS is a revolutionary approach designed to resolve joint C2 interoperability issues and evolve incompatible, Service-specific C2 programs into a single integrated C2 system. Figure 3-2 depicts GCCS.

3201. Background

The Assistant Secretary of Defense (C3I) and the Joint Staff are exercising oversight of GCCS implementation. The Assistant Secretary of Defense

(C3I) established the GCCS as the principal migration path for defense-wide C2 systems, directing that GCCS rapidly and efficiently deliver mission-essential C2 capabilities to combatant commanders through maximum use of commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) components. Further, he specified that the program evolve through a continuous requirements-refinement process to meet the goal of providing responsive C2 support to combatant commanders.

GCCS provides a fused and shared picture of the battlespace together with the essential planning and assessment tools required by combatant commanders and their subordinate commanders.

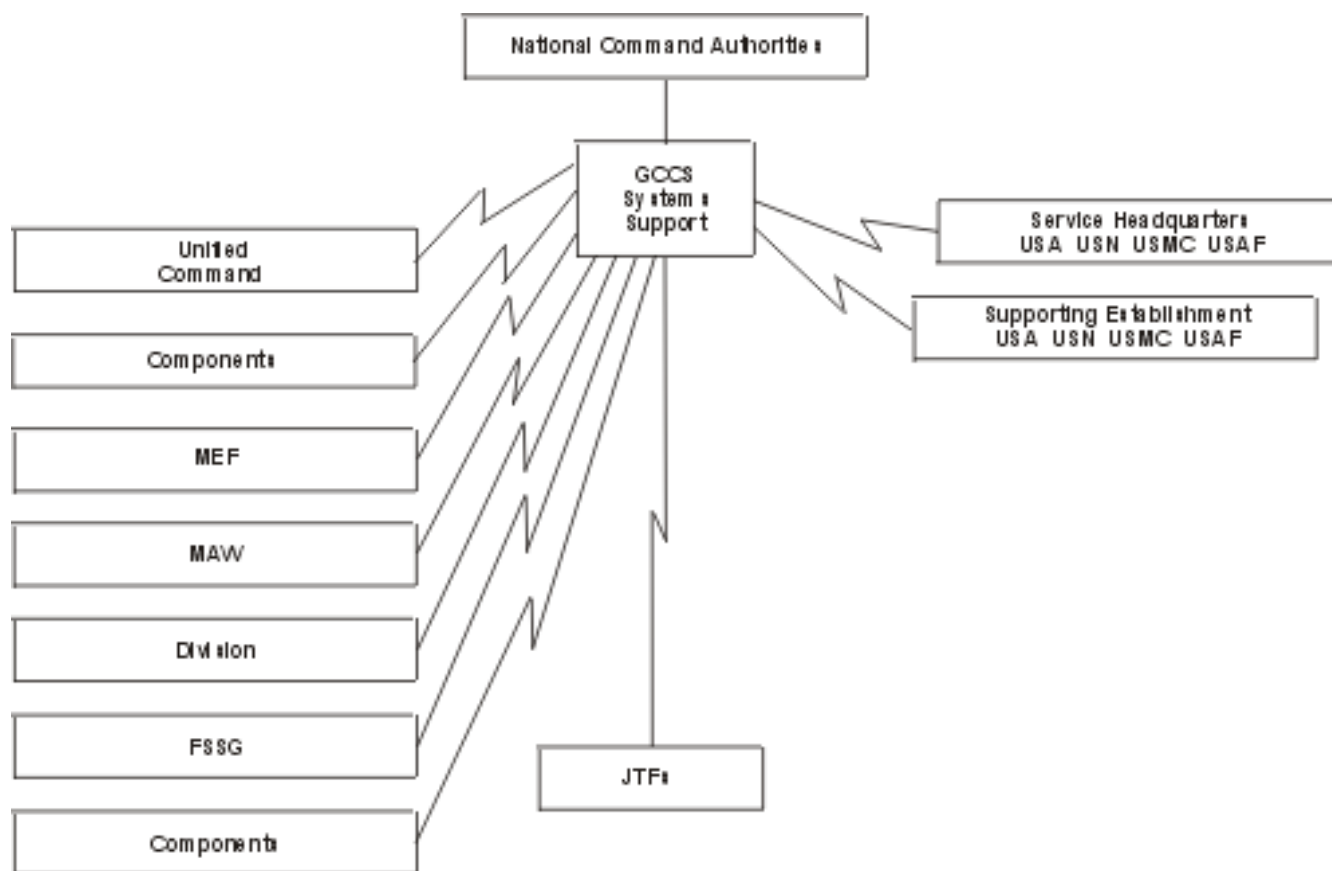


Figure 3-2. GCCS

GCCS also supports readiness assessment and reporting by the Services. GCCS employs a modern client-server architecture using commercial, open systems standards and will, through the ongoing DOD migration strategy, reduce the large number of information systems in use today.

GCCS is evolving from a baseline of existing C2 systems. This baseline has served as the cornerstone for the rapid implementation of an initial system capable of fulfilling the most critical user requirements. As new GCCS versions are subsequently fielded, existing legacy systems will be replaced. The common functional, physical, and operational characteristics of GCCS are based on a single COE described below. All future joint and Service/CINC-specific C2 systems must be compatible with this COE. The goal is to achieve a fully integrated, single GCCS in which all C2 functions are provided through GCCS application programs that have a common look and feel.

3202. Description

GCCS is composed of several mission application programs built within a single COE. GCCS also includes the network that supports sharing, displaying, and exchanging information. The GCCS infrastructure consists of a client-server environment incorporating UNIX-based servers and client terminals as well as microcomputer workstations operating on a standardized LAN. (Although GCCS currently employs a UNIX-centric architecture there is movement toward an architecture that exploits the capabilities of Windows NT. This is discussed in paragraph 3003.)

The GCCS infrastructure supports data transfer among workstations and servers. Connectivity between GCCS sites is provided by the secret internet protocol router network (SIPRNET), the secret layer of the DISN that is discussed in the next chapter. Remote user access is also supported by using dial-in communications and the telecommunication network (TELNET) protocol. Ultimately, GCCS will be able to operate in a multilevel security mode. See chapter 7 for more information on multilevel security initiatives.

The baseline GCCS architecture consists of a suite of relational database servers and application servers. At most GCCS sites, the relational database server acts as a typical file server by hosting user accounts, user-specific data, and site-specific files that are not part of GCCS. The application servers host the automated message handling system, applications not loaded on the database server, and other databases. At each GCCS site, one application server is configured as the executive manager. This server acts as the user interface and provides access to GCCS application programs through user identification and discrete passwords. GCCS software application programs are categorized into two groups: COE applications and mission applications.

Several key GCCS mission applications are described in paragraphs 3203 through 3211. GCCS is an evolutionary program with mission applications being added or improved in each new software release. The GCCS configuration management website (http://spider.osfl.disa.mil/new_home/cnfgmgmt/cnfgmgmt.html) contains detailed information on the current status of GCCS mission applications.

3203. Joint Operation Planning and Execution System

JOPES is the integrated C2 system used to plan and execute joint military operations. It is a combination of joint policies, procedures, personnel, and training and a reporting structure supported by automated data processing on GCCS. The capabilities of the JOPES mission applications support translation of the National Command Authorities' policy decisions into planning and execution of joint military operations. These applications are used by MAGTF planners for deployment and employment planning.

3204. Global Reconnaissance Information System

The Global Reconnaissance Information System supports the planning and scheduling of monthly

sensitive reconnaissance operations (SRO) theater requests. The Joint Staff staffs these requests through the Office of the Secretary of Defense, the Central Intelligence Agency, and the State Department for National Security Council approval. Incoming reconnaissance 1/2/3/4 formatted messages are received by an automated message handling system, validated, and passed to the Global Reconnaissance Information System application for automated processing and database update. The Global Reconnaissance Information System generates all reconnaissance messages and also monitors the monthly execution of theater reconnaissance missions approved in the previous month. The Global Reconnaissance Information System is used by the Joint Staff and theater commands exercising OPCON over airborne reconnaissance assets.

3205. Evacuation System

The Evacuation System collects and displays information about U.S. citizens located outside the United States as collected by U.S. State Department embassies and consulates. It accesses the database server via TELNET from a GCCS-compatible client.

3206. Fuel Resources Analysis System

The Fuel Resources Analysis System provides fuel planners with an automated capability for determining supportability of a deliberate or crisis action plan and for generating the time-phased bulk petroleum, oil, and lubricants required to support an operation plan (OPLAN). The Fuel Resources Analysis System facilitates review of the fuel requirements of a proposed, new, or revised OPLAN and assesses adequacy of available resources to support crisis action planning. Requirements can be generated and analysis performed either for the overall OPLAN, or by Service, or by region within the AO. Two or more OPLANs can be combined into a single OPLAN for analysis. The requirements generated can be varied through the use of intensity tables and consumption data extracted from the Logistics Fac-

tors File or with the Service-provided data system.

3207. Global Status of Resources and Training System

The Global Status of Resources and Training System provides information on the status of units with respect to personnel, equipment, and training. Query and display capabilities include categories of units (ships, fighter aircraft, ground forces, etc.), specific types of units (frigates, armor battalions, F-15 squadrons, etc.), and a specific unit (displays detailed status information).

3208. Theater Analysis and Replanning Graphical Execution Toolkit

TARGET contains a set of planning tools designed to support the operational planner during crisis action procedures. These tools allow planners and operators to accomplish tasks through rapid access to required documents; information sources; and analysis, multimedia, and teleconferencing tools.

3209. Joint Deployable Intelligence Support System (JDISS)

JDISS applications provide access to national, theater, and tactical intelligence sources through the joint architecture for intelligence. It provides protocols for connectivity and interoperability with intelligence systems required to support forces during peacetime, crisis, and war.

JDISS includes the protocols to access intelligence link (INTELINK) at the secret classification level (INTELINK-S). INTELINK-S is an intelligence dissemination service that enhances the sharing of intelligence information electronically over the SIPRNET. INTELINK provides intelligence dissemination by using networked informa-

tion discovery, retrieval, and browsing services. Its “point and click” technology makes intelligence products widely available to both users and producers of intelligence. JDISS applications are able to exchange sensitive compartmented information (SCI)—video and data—using the Joint Worldwide Intelligence Communications System (JWICS). The JWICS communications network is discussed in chapter 4.

3210. ATO

The ATO application provides the capability to view and print selected portions of ATOs. A query function allows the user to tailor requests for information in a specified order for viewing. The query function also supports the display of color-

coded ground tracks for selected portions of the order. ATO interfaces with the contingency theater automated planning system (CTAPS) and its follow-on theater battle management core systems (TBMCS).

3211. JMCIS

JMCIS is the foundation for the GCCS fused operational battlespace picture. It displays near real-time ground, sea, and air tracks. JMCIS uses a core service known as unified build to provide geographic display, contact correlation, and track database management. JMCIS Unified Build served as the basis for the original GCCS COE, which has evolved into the DII COE.

Section III

MAGTF C4I

MAGTF C4I is the concept for the integration of Marine Corps tactical information systems and the migration of selected systems to the DII COE. The MAGTF C4I concept is consistent with DOD mandates for DII compliance and designation of standard migration systems. MAGTF C4I provides commanders and their staffs at all levels of the MAGTF with the capability to send, receive, process, filter, and display data to aid them in their decisionmaking process. MAGTF C4I also provides a shared situational awareness through a common picture of the battlespace.

3301. Migration Strategy

The MAGTF C4I migration strategy focuses on incorporating the software functionality of MAGTF tactical information systems into a MAGTF C4I Software Baseline. Standard software mission applications and the capabilities to support MAGTF C2 functions are described and developed under the MAGTF C4I Software Baseline Program. The MAGTF C4I Software Baseline relies on the DII COE to provide its common software environment. The MAGTF C4I Software Baseline is developed using the DII COE software as its foundation. The MAGTF C4I Software Baseline configuration is coordinated with and controlled under the JMCIS Unified Build and DII COE programs. This strategy is based on the following:

- Integration with the DOD GCCS. No functionality offered by GCCS will be duplicated by the MAGTF C4I Software Baseline. All MAGTF C4I Software Baseline functionality that has joint applicability will be nominated for use by GCCS.
- Commitment to the DII COE and the evolution to open systems, including Windows NT®, Windows 95®, and Java®.

- Pursuit of a naval architecture that integrates USMC, Coast Guard, and Navy requirements.
- Focus on support of naval expeditionary forces in a joint environment.
- Pursuit of nondevelopmental items (NDI), COTS and GOTS solutions.
- Exploitation of Windows NT® to avoid the technical complexity and high costs associated with developing, integrating, operating, and maintaining UNIX-based systems.

3302. MAGTF C4I Software Baseline Capabilities

Table 3-1 (on pages 3-8 and 3-9) describes the current capabilities of the MAGTF C4I Software Baseline. Capabilities are added as new segments are approved and incorporated into the MAGTF C4I Software Baseline. As more capable segments are added, many older segments will be eliminated. These upgrades will occur continually as new releases of the MAGTF C4I Software Baseline are fielded to the FMF.

3303. Hardware/Operating System Requirements

MAGTF C4I Software Baseline uses Marine common hardware suite (MCHS) equipment, including the Hewlett-Packard TAC-4, CHS-2 Sun SPARC 20, and Intel PC platforms running the DII COE. The MAGTF C4I Software Baseline is completely transportable across the GCCS hardware platforms. These systems are certified through the security accreditation process in accordance with current DISA requirements. Various SECNAVINSTs provide guidance on security certification and accreditation procedures within the Department of the Navy (DON).

Table 3-1. MAGTF C4I Software Baseline Capabilities.

COE	
<i>Segment</i>	<i>Description/Purpose</i>
Universal Applications	
Windows NT	Application programming interfaces for mapping, communications, track database, and alerts from command and control PC and UNIX DII COE code. It is the minimum set of application program interfaces required for NT DII COE development.
Plotter	Ability to plot a tactical map overlay of a user-specified area on an acetate sheet.
Symbols	This COE improvement provides the capability to display MIL STD 2525 symbols and overlays to the common operational picture/common tactical picture display.
Tactical Digital Information Link (TADIL) A/B	This COE improvement provides the capability to receive, parse, and display TADIL A and B tracks.
Tactical Communications Interface Module (TCIM)	Capability to exchange over-the-horizon (OTH)-Gold tactical messages over SCR via the TCIM modem using the Marine tactical systems protocol.
Command and Control PC	MS Windows NT client program that provides the capability to participate in the common operational picture and common tactical picture using an Intel PC.
Netscape	COTS World Wide Web (WWW) browser and e-mail. It will also provide Web page production and shared whiteboard collaboration tools. May replace the functionality of Internet News, Intelligence Relay Chatter, and JDISS.
MS Office	COTS package that provides advanced word processing, graphics, spreadsheet, presentation graphics, and scheduling capabilities.
WABI	Capability to run a subset of MS Windows 3.11 applications, including MS Office, on a UNIX workstation. It is also required to run MS Office.
Maneuver	
Position Location Information System (PLIS) and JPI	Capability to receive, parse, and inject tracks into the track database from global positioning system (GPS) and other position location information (PLI) systems.
Routes	Graphical route planning tool with an overlay builder and trafficability analysis.
Intelligence	
MIG	Centralized database server for intelligence databases. Provides access to the National Information Database. Tactical data can be accessed, output, and updated by analysts at local and remote locations. Naval Intelligence Processing System (NIPS) applications are resident in MIG. NIPS also provides capabilities to process and store message traffic from various sources, generate and transmit messages, and create briefings with mapping and imagery tools.
Communications	
System Planning, Engineering, and Evaluation Device (SPEED)	SPEED applications will be available in the MAGTF C4I Software Baseline when converted to operate in Windows NT.
Strategic and Operational	
Air Field	Worldwide database of airfield capabilities by individual location.
TARGET	Timeline-based, time-phased force deployment data (TPFDD) editing and analysis tool.

Table 3-1. MAGTF C4I Software Baseline Capabilities (continued).

COE	
<i>Segment</i>	<i>Description/Purpose</i>
Evacuation System	Database of potential evacuees at foreign service posts.
Force Augmentation Planning and Execution System (FAPES)	OPLAN mobilization planning, analysis, and execution tool.
Fuel Resources Analysis System	OPLAN fuel capacity, requirement, and expenditure tool.
GCCS ATO Review (GARC)	ATO confirmation message browser. Data is parsed from messages sent by CTAPS. May duplicate the NIPS functionality for Sun SPARCs.
Global Status of Resources and Training System	Tool to enter status of unit locations, deployment readiness, and training.
Global Transportation Network (GTN)	Visibility into USTRANSCOM transportation data for the global transportation network.
Individual Manpower Requirements and Availability System (IMRAS)	Individual mobilization planning and execution tool.
Imagery Product Archive (IPA)	Imagery files and products database.
Internet News	SIPRNET bulletin board tool.
Intelligence Relay Chatter	SIPRNET chat tool.
JDISS	Multimedia applications used to access intelligence information databases over INTELINK and other networks.
Joint Engineer Planning and Execution System (JEPES)	OPLAN civil engineering tool.
JOPES: Ad Hoc Query	Ad hoc querying capability to the JOPES using data fields and Boolean operators from a pick list. May duplicate the NIPS ad hoc functionality.
JOPES: Information Resource Manager (IRM)	Generic database manipulation tool for compositing OPLANs.
JOPES: JOPES Navigation (JNAV)	JOPES front-end tool.
JOPES: Predefined Reports (PDR)	JOPES OPLAN report tool.
JOPES: Requirement Development Analysis (RDA)	JOPES TPFDD force module generator.
JOPES: Scheduling and Movement (S&M)	JOPES TPFDD scheduling and movement tool.
Logistics Sustainment Analysis and Feasibility Estimator (LOGSAFE)	Logistics sustainment, feasibility, resupply requirements, contingency plans, and “black-bottom” cargo transportation tool.
Medical Planning and Execution System (MEPES)	OPLAN medical requirements tool.
Oracle	COTS relational database management system that provides access to the various databases within the system. It allows the users to access, query, and update information in the databases. May duplicate the NIPS Sybase functionality.

Although the MAGTF C4I Software Baseline maintains UNIX operating system segments, new development is based on Windows NT. The UNIX-based TAC-4 and CHS-2 platforms are interim application and data servers. However, both IAS and TCO workstations are transitioning to a common PC-based Windows NT® environment.

All systems will be DII COE/MAGTF C4I compliant. All systems will operate on the standard MCHS of equipment and will be distinguished only by the set of applications or functional segments resident on the computer. The Marines that use each of the functional area tactical data systems (TDS) in this section are responsible for setting up, operating, and maintaining those systems (e.g., Marines from the G-3/S-3 will be responsible for setting up, operating and maintaining TCO and Marines from the G-2/S-2 will have those responsibilities for IAS). CIS personnel will assist these functional users in the operation and maintenance of their systems and provide external network connectivity and IP addresses. This division of responsibilities requires close cooperation and coordination between the functional system user and CIS personnel and applies to all of the information systems described in this section. System descriptions in paragraphs 3304–3309 are organized by the functional area that they support.

3304. Maneuver

Maneuver systems support operations planning and execution by providing commanders and staffs with shared situational awareness through an integrated representation of the battlespace. Maneuver systems pull and fuse information from all functional areas. These systems provide the means for mission receipt and rapid development and dissemination of the commander's intent and OPLANs and OPORDs.

The tactical combat operations (TCO) system provides an automated capability to process battlefield information. TCO provides timely information to help commanders and their staffs conduct operations planning and make critical C2 decisions. TCO processes and fuses tactical information to form a common picture of the battle-

field. TCO supports the development of COAs and the preparation and dissemination of OPLANs and OPORDs, including overlays that are geographically referenced to an electronic map.

TCO supports the operations sections of all FMF units of battalion/squadron size and larger as well as planning sections at higher echelons. TCO consists of computer workstations operating at the secret level on multiple LANs interconnected on the SIPRNET through MAGTF communications networks. TCO components include the MCHS terminals, the tactical communications interface module (TCIM) for radio interface, and LAN equipment. The functional manager for TCO is the G-3/S-3, and COC personnel are responsible for setting up the TCO equipment in their operations centers. Communications and information systems personnel are responsible for connecting TCO terminals to the SIPRNET, providing them with IP network host addresses, and assisting operations COC personnel in installing and maintaining the TCO.

JMCIS-Afloat and TCO are both built around the JMCIS Unified Build core software. This permits Marine forces embarked aboard Navy ships to “plug in” to the JMCIS-Afloat. Furthermore, because the JMCIS Unified Build served as the baseline for the DII COE, migration of TCO to the DII COE is occurring rapidly. DII COE compliance will provide complete interoperability with GCCS and other DII COE compliant systems.

3305. Intelligence

Intelligence systems support the timely planning, collection, processing, production, and dissemination of all-source intelligence. In addition, these systems support the effective employment of reconnaissance, surveillance, and target acquisition resources.

a. IAS

Intelligence analysis system (IAS) provides MAGTF intelligence personnel with intelopera-

tions planning and direction, all-source processing and fusion, and dissemination capabilities. IAS is the principal Marine Corps intelligence information system. The G-2/S-2 is the functional manager for IAS, and intelligence personnel are responsible for setting up IAS equipment in their intelligence centers. MEF IAS is a sheltered, mobile system with multiple (scalable) analyst workstations in a client-server LAN configuration. IAS suites for intermediate commands are configured in a four-workstation LAN. Single IAS workstations support battalions and squadrons. IAS uses MCHS equipment and will transition to the DII COE. IAS hosts the secondary imagery dissemination system (SIDS), and links are planned with other intelligence systems at the national (DOD Intelligence Information Systems [DODIIS]), theater, and tactical (including TCAC, Tactical Electronic Reconnaissance Processing and Evaluation System (TERPES), and Joint Services Imagery Processing System [JSIPS]) levels.

b. MAGTF SIDS

The manpack SIDS device provides the capability to electronically collect, transmit, and receive imagery products throughout the MAGTF, as well as through adjacent, higher, and external commands. MAGTF manpack SIDS uses MAGTF communications networks and complies fully with the national imagery transmission format (NITF) Version 2.0 and the Tactical Communications Protocol (TACO II). MAGTF SIDS is fielded in two configurations. One configuration is hosted on the IAS; the other is a standalone manpacked configuration. Both configurations allow the user to display, manipulate, annotate, print, transmit, and receive images on a multipurpose workstation.

c. TCAC Product Improvement Program

Tactical control and analysis center product improvement program (TCAC PIP) provides the radio battalions with a fully capable SIGINT processing, production, and dissemination system (and other C2 information systems) that is shelter-mounted on a heavy variant, high-mobility, multipurpose wheeled vehicle (heavy HM-MWV). The TCAC PIP includes three SUN

workstations, two SUN servers, and five radios (one HF, two VHF, one UHF, and one UHF satellite communications [SATCOM]). Through its automated processing, analysis, and reporting capability, TCAC PIP enhances the overall control and management of SIGINT assets as well as the development and dissemination of SIGINT products. Timely, fused, and filtered SIGINT products are provided to MAGTF commanders, usually through the MAFC.

d. Joint Surveillance Target Attack Radar System

The JSTARS aircraft is a U.S. Air Force asset that can provide the MAGTF commander with a near-real-time depiction of the surveillance area for intelligence and battlespace situational awareness. JSTARS detects and tracks moving and stationary ground targets in the AO, including data on enemy forces and position location of friendly forces. Access to this theater asset also enhances target acquisition and identification, postattack combat assessment, indications and warning, cueing/cross-cueing among intelligence collectors, operations planning and execution, and pattern analysis/intelligence fusion.

JSTARS consists of two major components: the U.S. E-8C aircraft and the common ground station (CGS), which provides connectivity to the aircraft. The sensor suite provides target detection and tracking through moving target indicator, fixed target indicator, and synthetic aperture radar data. The aircraft transmits data sets to the CGS via a surveillance control data link. The CGS terminates the surveillance control data link and processes and manipulates the sensor data sets. Map data are registered and topographical features entered on the two operator workstations and digitized plotting boards within the CGS. The JSTARS picture will be fed simultaneously from up to four CGS remote workstations, which may be located in the MAFC, the current operations cell, the FFCC, the future operations cell, or other C2 nodes. The MAFC serves as the principal C2 node for correlating, analyzing, and interpreting JSTARS information and for its dissemination to MAGTF subordinate units.

In the future, full JSTARS data sets (moving target indicator, fixed target indicator, and synthetic aperture radar imagery), fused intelligence, track database information, and contact and track data information will be available throughout the MAGTF down to regimental/MAG levels via IAS, TCO, and/or the Advanced Field Artillery Tactical Data System (AFATDS) by using the TDN backbone.

e. Mobile Electronic Warfare Support System Product Improvement Program

The MEWSS, mounted in an LAV, provides SIGINT/EW support to a wide variety of missions, including LAR operations. The MEWSS PIP provides the radio battalions with an upgraded SIGINT/EW suite. The MEWSS PIP is a wide-band intercept system that provides a complete picture of the enemy electronic order of battle and state of the art electronic warfare support measures (ESM). The system contains three primary mission subsystems that are also part of the Army's Intelligence/EW Common Sensor program.

The primary mission subsystems consist of a communications intelligence (COMINT) system that provides intercept, collection, and geolocation across a broad frequency range and a capability against a variety of modern threat communications emitters; an electronic intelligence (ELINT) system that provides interception, identification, and geolocation of noncommunications emitters, including counterbattery and battlefield radar; and a precision location system to locate communications emitters to within targeting accuracy. The MEWSS PIP system includes an electronic attack (EA) module that is capable of "smart" and conventional jamming. The MEWSS PIP is completely interoperable with Army Intelligence/EW Common Sensor platforms, thereby allowing cooperative engagement and data sharing.

f. TERPES

Tactical Electronic Reconnaissance Processing and Evaluation System (TERPES) is a system that supports the reception, processing, evaluation,

and dissemination of electronic reconnaissance information. Data is received from EA-6B aircraft by data links, magnetic tape, and crew logs. TERPES also supports EA-6B mission planning, briefing, and debriefing and generates intelligence for strike mission planning. TERPES fuses data from EA-6B missions with information from other national and theater sources to update the electronic order of battle and passes intelligence to the IAS for further processing and dissemination. TERPES is housed in one 8-foot by 8-foot by 20-foot shelters dedicated to mission analysis, mission planning, and mission support.

3306. Air Operations

Air operations systems support the planning, coordination, and control of MAGTF air combat operations and interface with Navy, joint, and combined forces air operations systems. These systems also interface directly with fire support systems.

The MACCS provides the tactical air commander with the automated support required to exercise control over MAGTF air operations. MACCS supports tactical air command, tactical air operations, air defense, and direct air support. Personnel dedicated to these systems provide support for their installation, operation, and maintenance. The MWCS provides the multichannel communications connectivity that links the airfields and forward sites, as well as the long haul single channel radio support between higher and adjacent commands and the wing headquarters and TACC.

a. Tactical Air Command Systems

Tactical air command systems provide the tactical air commander with support for planning, controlling, and coordinating overall MAGTF air operations. Functions supported include determination of operational requirements, allocation of aircraft, publication of ATOs, planning of air operations, coordination and supervision of execution, and coordination with naval and joint agencies. CTAPS, one of the mission applications supporting tactical air command, is used to create and disseminate the ATO. The Joint Chiefs of Staff

have mandated the use of CTAPS for joint ATO dissemination. CTAPS runs at the secret level on UNIX-based MCHS servers on the TACC LAN. The MWCS provides each CTAPS workstation with an IP host address and connects the TACC LAN to remote airfields, DASC, TAOC, and other Service command centers over SIPRNET by using IP routers and organic transmission assets. Tactical air command systems are evolving to provide improvements in a number of areas, including migration to common hardware and DII COE compliance, mobility, and Joint Tactical Information Distribution System (JTIDS) integration. Through such enhancements, tactical air command systems will provide the automated tools needed to effectively plan, coordinate, and direct all MAGTF tactical air operations.

b. Air Defense Systems

The Tactical Air Operations Center (TAOC) is the C2 agency that controls tactical air operations and coordinates the air defense of the MAGTF. The TAOC consists of the AN/TYQ-23(V)1 Tactical Air Operations Module (TAOM) and associated sensors, the AN/TPS-59, AN/TPS-63, and its replacement, the AN/MPO-62 radars, and the sector antiair warfare facility. The TAOM provides automated support for surveillance, weapons control, air traffic control, and training. The operator console of the TAOM is being upgraded to provide GCCS functionality and a Windows interface. The Sector Antiair Warfare Facility provides the tactical air picture from the TAOM to the sector antiair warfare coordinator and enables an automated interface between CTAPS and TAOM for passing the ATO. JTIDS implementation is ongoing and will provide greatly enhanced, secure, high-capacity, jam-resistant information distribution capabilities as well as improved interoperability for the conduct of joint air defense and theater missile defense operations.

c. Direct Air Support Systems

The high-mobility downsized DASC provides automated support to the DASC for the conduct of air operations directly supporting ground forces. It provides support for the coordination of close air strikes, assault support, and air reconnaissance missions. The high-mobility downsized DASC is

an integrated system that consists of five lightweight multipurpose shelter Type-1 systems mounted on M-1097 heavy HMMWVs. Each operations shelter contains five operator workstations capable of conducting integrated aviation C2 functions. Each high-mobility downsized DASC vehicle tows an M-116 trailer that carries a generator and external cables. The trailers associated with the operations suites also carry one quick-erect shelter. The system design allows for maximum employment flexibility to support any level of MAGTF operations, providing the FMF with a lightweight, highly mobile system that is capable of responsive direct air support C2.

3307. Fire Support

Fire support systems support the planning, coordination, and control of artillery, air, and naval gunfire.

a. Fire Support Command and Control System (FSC2S)

The FSC2S is designed to meet the basic requirements for a fully automated fire support system. It provides initial semiautomated tactical fire support and technical artillery fire control functions for MAGTF operations. The follow-on AFATDS completes the transition to fully automated fire support C2. There are two components to the FSC2S: the fire control system and the battery computer terminal.

The FSC2S is employed at FDCs down through the firing battery level, at FSCCs down through the battalion level, at the SACC, and by the MAGTF CE to support fire planning and tactical fire direction. The FSC2S is supported by digital fire support communications nets.

b. Advanced Field Artillery Tactical Data System (AFATDS)

The AFATDS is a joint Army/Marine Corps system which will replace the initial fire support automated system (IFSAS). It is a multi-service, integrated, battlefield management and decision support system which incorporates automation into the fire support warfighting function to assist

the commander in the planning, delivery, and coordination of supporting arms. These terminals will be located in FSCCs, DASC, TACC, and artillery battalion and regimental FDCs. AFATDS will provide the MAGTF commander with the capability to rapidly integrate ground, air, and naval surface fire support with the scheme of maneuver. The AFATDS software architecture is interoperable with Marine Corps CIS, GCCS COE, and MAGTF C4I baseline systems.

3308. Logistics

LOG systems support logistic planning and operations. These include all logistic functions supporting deployment, employment, and reconstitution of forces.

There are two basic uses for information: to promote situational awareness as the basis for a decision and to direct and to coordinate actions in the execution of that decision. There are currently over one hundred logistic information systems utilized within the Marine Corps to support Force Deployment Planning and Execution, sustainment and distribution. Biannually, the Installations and Logistics Department, Headquarters Marine Corps publishes a comprehensive listing of these systems in a Logistics Information Resources Plan (Log IR Plan). The Log IR Plan provides a roadmap for how logistics information systems will utilize information technology methods. It also provides a migration strategy that tailors the number of systems by eliminating redundancies and leveraging joint systems where appropriate. While by no means a complete listing, the following provides a top down view of the significant of information systems currently in use to support force structure, movement, sustainment, materiel readiness, and fiscal management.

a. Systems in Support of Operations

(1) Standard Accounting, Budgeting, and Reporting System (SABRS). SABRS is a DOD automated system used by Marine Corps fiscal planners to account for and report expenditures of appropriated funds and for use in submissions to the DOD budget cycle.

(2) MAGTF II/Logistics Automated Information System (LOGAIS). This family of systems supports Marine Corps ground logistic data requirements. The MAGTF II system is the primary planning tool for selecting and tailoring a MAGTF and for providing updates to JOPES to support FDP&E. It includes TC-AIMS and MDSS II. TC-AIMS II, a joint system, will eventually replace TC-AIMS and MDSS II. TC-AIMS and ATLASS will be the primary systems that provide functional logistics management for sustainment and distribution.

(3) Transportation Coordinators' Automated Information for Movement System (TC-AIMS). TC-AIMS provides automated support for motor transport control, planning of support, and coordination of overland movement and convoys. It manages use and movement of day-to-day motor transport and heavy equipment. Its resource-management module provides inventory, support requests, and task and dispatch management. It supports convoy management with an embarkation and marshaling module. It tracks critical events, including user time statistics. TC-AIMS interfaces with the MAGTF Deployment Support System II (MDSS II). This system, along with TC-AIMS, assists in deployment planning and execution and unit movement at the MEF level and below. The integrated MAGTF/LOGAIS software will enable an improved degree of integration between MDSS II and TC-AIMS.

(4) Theater Medical Information Program (TMIP). TMIP provides a global capability that links medical information databases to integration centers; these integration centers are accessible to Navy medical personnel while engaged in support of Marine forces. The goal for TMIP is to provide theater medical integrated automated information using Global Command and Control System (GCCS) and Global Combat Support System (GCSS) that links all echelons of medical care in support of Marine forces.

(8) MDL. MAGTF Data Library is the data dictionary tool used to facilitate gathering of valid source data for use by all of the MAGTF/LOGAIS family of systems.

(5) MDL. MAGTF Data Library is the data dictionary tool used to facilitate gathering of valid source data for use by all of the MAGTF/LOG-AIS family of systems.

b. Systems in Support of Materiel Readiness

(1) Global Status of Resources and Training System (GSORTS). GSORTS provides information on the readiness status of units with respect to personnel, equipment, and training.

(2) Asset Tracking Logistics and Supply System (ATLASS). ATLASS provides automated support for supply and maintenance. It replaces two mainframe-based systems developed in the early 1970s—the Marine Integrated Maintenance Management System (MIMMS) and the Supported Activities Supply System (SASSY)—with a client-server system based on an open systems architecture. ATLASS is being implemented through phased development, with the current phase focusing on integrating user-unit supply and shop-level maintenance functions.

(3) Naval Tactical Command Support System. NTCSS is a fleet tactical command support system used by the ACE. NTCSS replaces 1970s vintage fleet equipment with modern minicomputers, personal computers, and local area networks. It provides status and ad hoc reports to the Battle Group Logistics Coordinated Support System (BGLCSS). The system is formulated around SNAP III, which began the process of integrating shipboard computers by adopting the command and control systems architecture for command support applications.

(4) Shipboard Nontactical ADP Program III (SNAP III). The Marine wing support group (MWSG) and MALS use SNAP III hardware to provide automated information processing support for supply, finance, and organizational maintenance management.

(5) Naval Aviation Logistics Command Management Information System (NALCOMIS). MWSG and MALS use the NALCOMIS software application to provide automated information pro-

cessing support for maintenance of all aviation equipment and spares to aviation units and selected base and garrison activities throughout the Marine Corps.

(6) Shipboard Uniform Automated Data Processing System (SUADPS). This is the supply software application used by MALS to provide financial, inventory, and logistic management of aviation supply support for Marine aircraft.

(7) Conventional Ammunition Integrated Management System (CAIMS). CAIMS provides on-line inventory management data such as ammunition location, quantity, material condition, purpose code, and requisition status.

3309. Force Deployment Planning

Force deployment planning systems support planning for the movement of forces and their sustainment from original locations to specified operational areas. The MAGTF II system supports deployment planning. It enables Marine deployment planners to conduct both deliberate and time-sensitive (crisis action) planning. By using MAGTF II, planners can select and tailor MAGTFs and estimate sustainment and lift requirements. MAGTF II is a PC-based system that supports TPFDD development and maintenance, with the results uploaded to JOPEs. MAGTF II can operate on a LAN, although system users and administrators must be mindful of security concerns. Because of its usability, versatility, and portability, MAGTF II has been nominated as a migration system that will, with specific modifications, serve all Services and the Joint Staff as an automated tool to support deployment planning and execution. For detailed information on force deployment planning, see Joint Pub 5-03.1, *Joint Operation Planning and Execution System*, Volume I.

The MAGTF C4I systems described above normally operate on LANs in various C2 facilities of the MAGTF. A notional layout of the systems that support COCs is in figure 3-3 (on page 3-16).

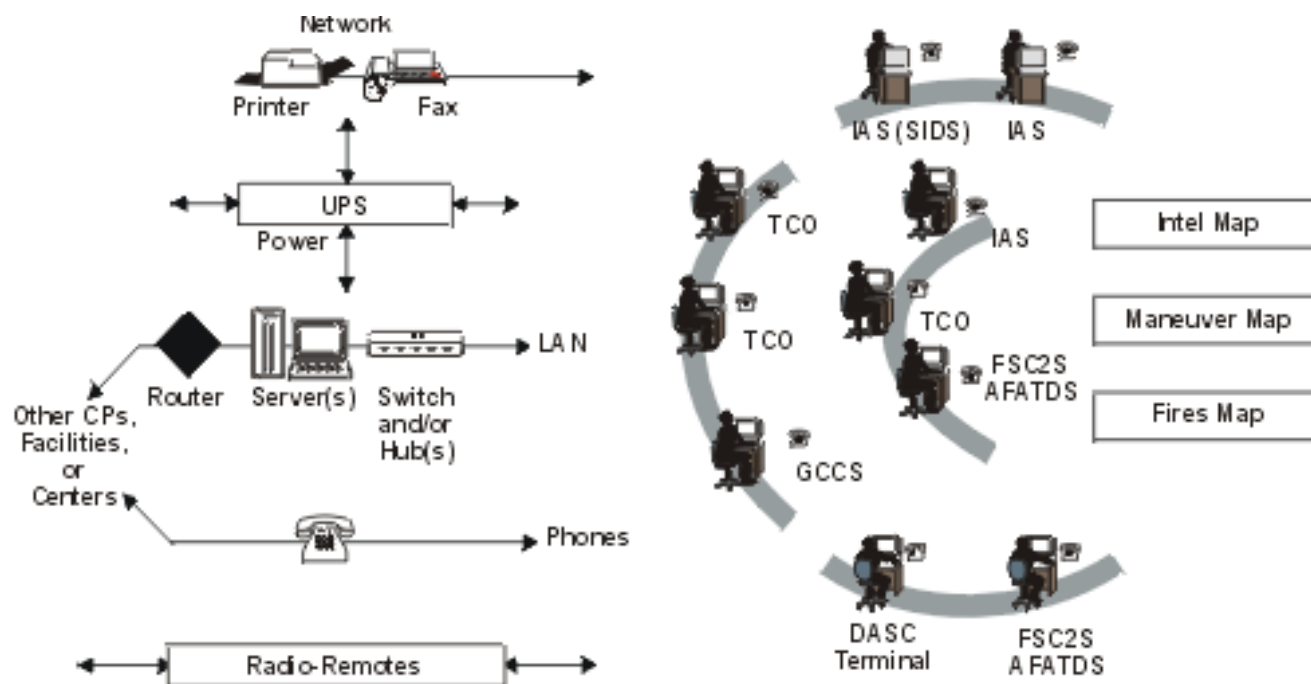


Figure 3-3. Supporting Systems.

Section IV

The Defense Message System

DMS is an evolving system that consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in the DOD. The current subsystems of the DMS are the automated digital network (AUTODIN) (which includes base-level support systems) and e-mail. DMS will have a store and forward capability. The DMS must support interfaces to systems of other government agencies, allies, tactical systems, and defense contractors. System users may be deployed or in garrison, fixed or mobile. The planned or objective system will replace the current subsystems, based on DOD standards, with a single system based on international standards established by the International Organization for Standardization (ISO). Security services, including authentication, integrity, confidentiality, and registration, are provided through the Fortezza Personal Computer Memory Card International Association (PCMCIA) card, which is discussed later in this chapter. The primary objective of the DMS is to maintain existing service and security while reducing cost and staffing.

3401. AUTODIN

The transition to the objective system involves replacing AUTODIN delivery systems and existing e-mail capabilities based on the simple mail transfer protocol (SMTP) with e-mail based on the ISO X.400 message handling protocol and the supporting X.500 ISO standard for directory services. The transition also involves transitioning the security and service management infrastructure. Final AUTODIN closeout is scheduled for 31 December 1999. Remaining non-DMS message

systems will be phased out and DMS capabilities will be upgraded by the end of calendar year 2008. Services and agencies have been tasked to develop transition plans for implementation of the new system and have been asked to include supported CINCs in their plans. DMS has been designated the single DOD message system and will be integrated with all applications that have embedded messaging functions, such as GCCS.

3402. Upgrades

Joint requirements, policy, doctrine, and architecture and a transition plan for interfacing and incorporating tactical users into the DMS are still under development. At present, tactical message traffic enters the long-haul network primarily through AUTODIN switching centers and automatic message processing exchanges. The AUTODIN interface into the DMS is scheduled to be phased out by 31 December 1999; therefore, the impact on tactical users, including the need to interoperate with legacy tactical message switches, will be felt over several years. The primary MAGTF message handling system replaced by DMS is the AN/MS-63A message switch. DMS also replaces VINES mail, a proprietary messaging system used throughout the Marine Corps. DMS will improve tactical messaging by providing a seamless system across the strategic and deployed environments. It provides a secure, timely, reliable writer-to-reader messaging service. The DMS program helps to integrate the tactical and strategic environments and is a key component of the DII. CJCSM 6231.03A, *Joint Data Systems*, provides additional detailed information about the DMS.

Section V

Information Services

Information management and exchange are supported not only by the information systems described previously, but also by common information services hosted on servers throughout the MAGTF. Many of these information services have already been mentioned as part of the DII COE and the MAGTF C4I Software Baseline. Figure 3-4 shows these services, which are described in the following paragraphs. These services enable the flow of information over the communications networks supporting the MAGTF.

Communications	Mission Application
Fax	File
Message	Database
Security/Firewall	Network Operating System
Defense Message System	Network Management
World Wide Web	Directory
Print	Domain Name
Network Administration	TELENET 3270

Figure 3-4. Information Services.

3501. Directory Services

Directory services consist of Marine Corps standard network directory service application, the domain name system (DNS), and X.500. The Marine Corps standard network directory service application is Banyan Street Talk Directory Assistance. As mentioned above, X.500 is the ISO standard for directory services that supports X.400 messaging and will be part of DMS. DNS is a directory service that links Internet domain names to the IP addresses specified by network administrators. The DNS organizes the names of hosts in a hierar-

chical fashion, much like a file system. The remainder of the domain name is administered by the network administrator of the subnetwork, and the subnetwork is often broken up into additional zones to ease administration. The network administrator is responsible for setting up name servers to handle requests for domain name-to-address resolution for the network administrator's zones.

3502. Terminal Emulation Services

Terminal emulation services provide the capability for remote users to access logistic and personnel applications hosted at DISA megacenters. Remote logins are supported through a synchronous terminal emulation using the TELNET protocol.

3503. Message Handling Services

Message handling services provide message storage, transfer, forwarding, routing, translation, and format conversion. Services include SMTP, multipurpose Internet mail extension (MIME), and ACP 123 message handling capability.

3504. Network Management Services

Network management services link a Network Management System and networked devices (e.g., servers) being managed. Network management is provided through the simple network management protocol (SNMP) Through SNMP the system administrator is alerted when traffic patterns and conditions indicate that a networked device is failing or has failed. A network manager can set thresholds for devices and receive an alarm when the threshold is reached.

a. Configuration Management

Configuration management includes resource servicing, testing, and reporting; software distribution and licensing; planning; and management. Configuration management also includes the planning and use of directories. Configuration management requires maintenance of complete records of users, assignments, equipment, and other information needed to administer the network. Planning support consists of development, dissemination, and coordination of letters of instruction, Annex K for OPLANs\OPORDs, routing tables, address assignments, and message handling instructions.

b. Fault Management

Fault management consists of fault determination, correction, prevention, reporting, and archiving. File server backup and recovery functions consist of providing backup and recovery services locally and from one server to another in the network.

c. Performance Management

Performance management consists of performance and traffic characterization, performance testing, performance timing and correction, control of performance management, reporting, and archiving.

d. Security Management

Security management consists of configuration management of security components, security mechanism management (including identification and authentication, discretionary access control, object reuse, and the use of audit trails), system vulnerability reduction, and other methods to prevent security breaches. Figure 3-5 (on page 3-20) is an outline of the interactions and relationships between the various MAGTF C4I services and protocols.

3505. Security Services

Information systems security is discussed in depth in chapter 7.

a. Fortezza Cards

The Fortezza card is a security component that provides user privileges for sending and receiving DMS messages. The Fortezza cards include private security keys and user messaging privileges. User messaging privileges include individual messaging and organizational message release, including organizational level, precedence, and classification authorized. Directory queries for DMS directory services are authenticated by the digital signature function of the Fortezza PC card to allow access to the X.500 directory. The Fortezza PC cards are programmed by using the certification authority workstation.

b. Certification Authority Workstation

The certification authority workstation is a PC-based application used to program and maintain Fortezza PCMCIA cards for users. These Fortezza cards (one per person) include not only private security keys, but also the user messaging privileges. Local authorities use the DMS agent software applications resident in the certification authority workstation to perform distributed directory and security management tasks. This trusted workstation supports functions that include decentralized assignment of directory names and creation of X.509 certificates. As part of this process, the applications initialize each user's Fortezza card with a personal identification number (PIN), X.509 certificate(s), and selected DMS information.

c. In-line Network Encryptors

In-line network encryptors use the Secure Data Network System standards from the National Security Agency and interface to the National Electronic Key Management System. In-line network encryptors provide end-to-end security between hosts and workstations running on secure LANs. In-line network encryptors allow secure communications over public, packet-switched, and unclassified backbone networks. In-line network encryptors incorporate an open architecture.

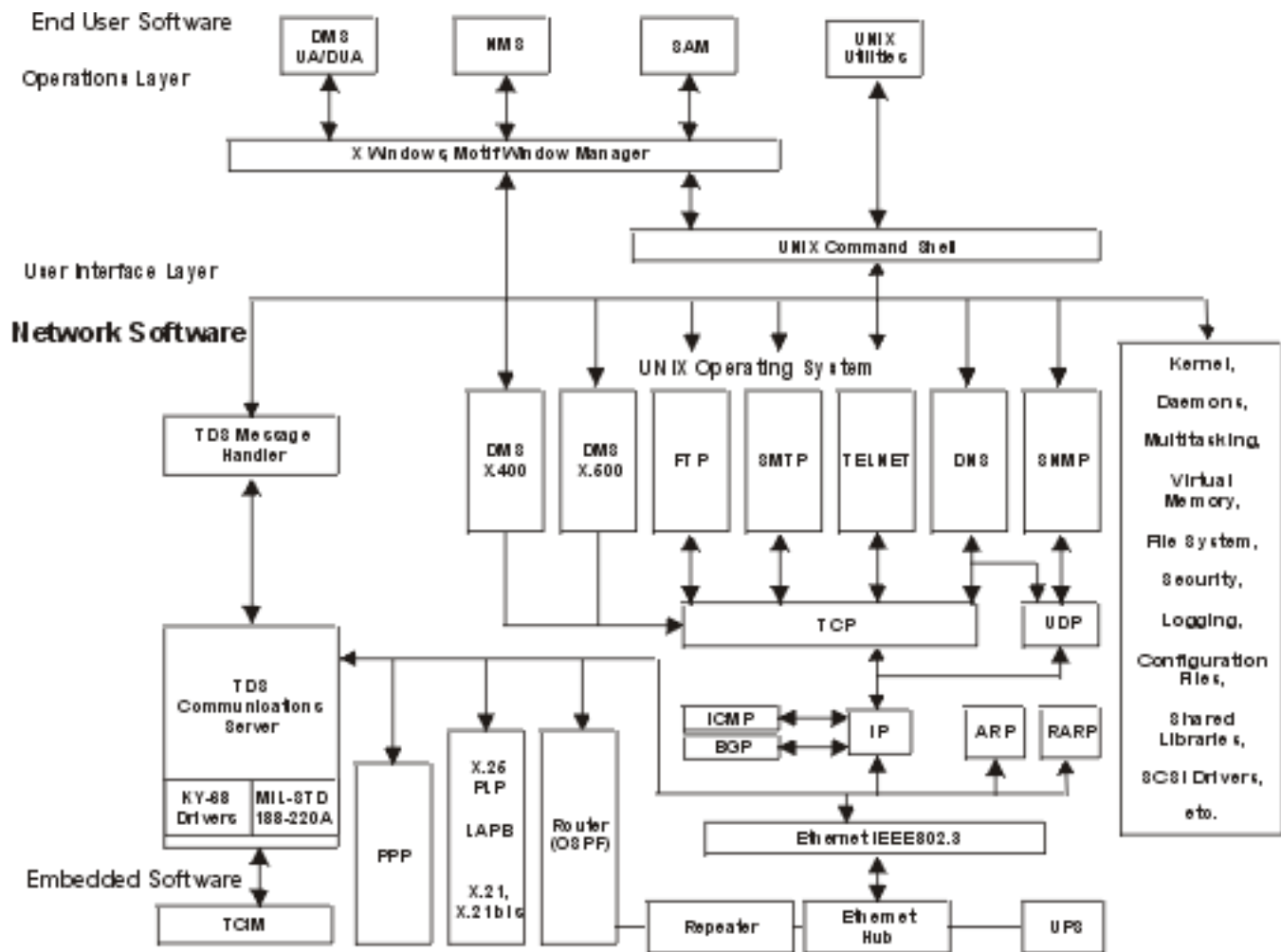


Figure 3-5. MAGTF C4I Services and Protocols.

3506. Facsimile Services

Facsimile services allow the sending and receiving of electronic text, graphics, and images through the switched telephone network. The facsimile server provides storage, routing, and translation of data.

3507. Communications Services

Communications services provide communications management between LANs and WANs.

This server provides dynamic addressing and routing services that allow automated selection of the pooled communications resources at a central location. It interfaces with the message handler and the TCIM to provide automated radio network message addressing and routing. This server supports Marine tactical systems, Transmission Control Protocol (TCP)/IP, e-mail, file transfer, SNMP, and SMTP.

Section VI

Shipboard Information Systems

Naval amphibious ships provide CIS support to embarked Marine forces as well as spaces from which to exercise command and control. Available shipboard information system support will seldom fully satisfy the requirements of the embarked Marine force and, consequently, will require augmentation by organic MAGTF information systems support resources.

3601. Key Resources

Appendix I is an overview of the various CIS resources available on amphibious ships. However, the actual CIS support available on amphibious ships varies, even between ships of the same class, based on system installation and upgrade schedules. Specific configurations, including identification of software release versions, must be determined during pre-deployment and embarkation planning. Figure 3-6 (on page 3-22) depicts the information systems and equipment typically available on amphibious ships, focusing on communications resources and LANs that are key to shipboard command and control.

3602. JMCIS-Afloat

JMCIS-Afloat (formerly known as Navy Tactical Command System-Afloat [NTCS-A]) provides the tactical commander with timely, accurate, and

complete all-source information management, display, and dissemination capabilities. These include multisource data fusion and distribution of command, surveillance, and intelligence data and imagery to support warfare mission assessment, planning, and execution. JMCIS-Afloat is DII COE compliant and shares the JMCIS Unified Build software with TCO. This commonality permits the MAGTF to operate TCO in the LFOC and the IAS in the JIC.

JMCIS-Afloat includes the NIPS database interface and the national, regional, and organic sensor intelligence and environmental databases. The JDISS and other services described in the GCCS section are also included in JMCIS-Afloat. Embarked MAGTF commanders can access and use the JMCIS-Afloat services by using MAGTF and/or shipboard computers (with prior coordination) on ships' LANs. Flagships such as CV, CVN, LHA, LHD, and LCC have been upgraded to the latest version of JMCIS, while most of the unit-level platforms such as CG, DD, DDG, LPD, LPH, and LSD ships are using older software versions that have incompatibilities with the MAGTF C4I Software Baseline. Upgrades are continual; until the Navy can achieve a coordinated simultaneous software update with the Marine Corps, this condition requires that MAGTF CIS personnel adapt and find ways to make the networks provide the required services.

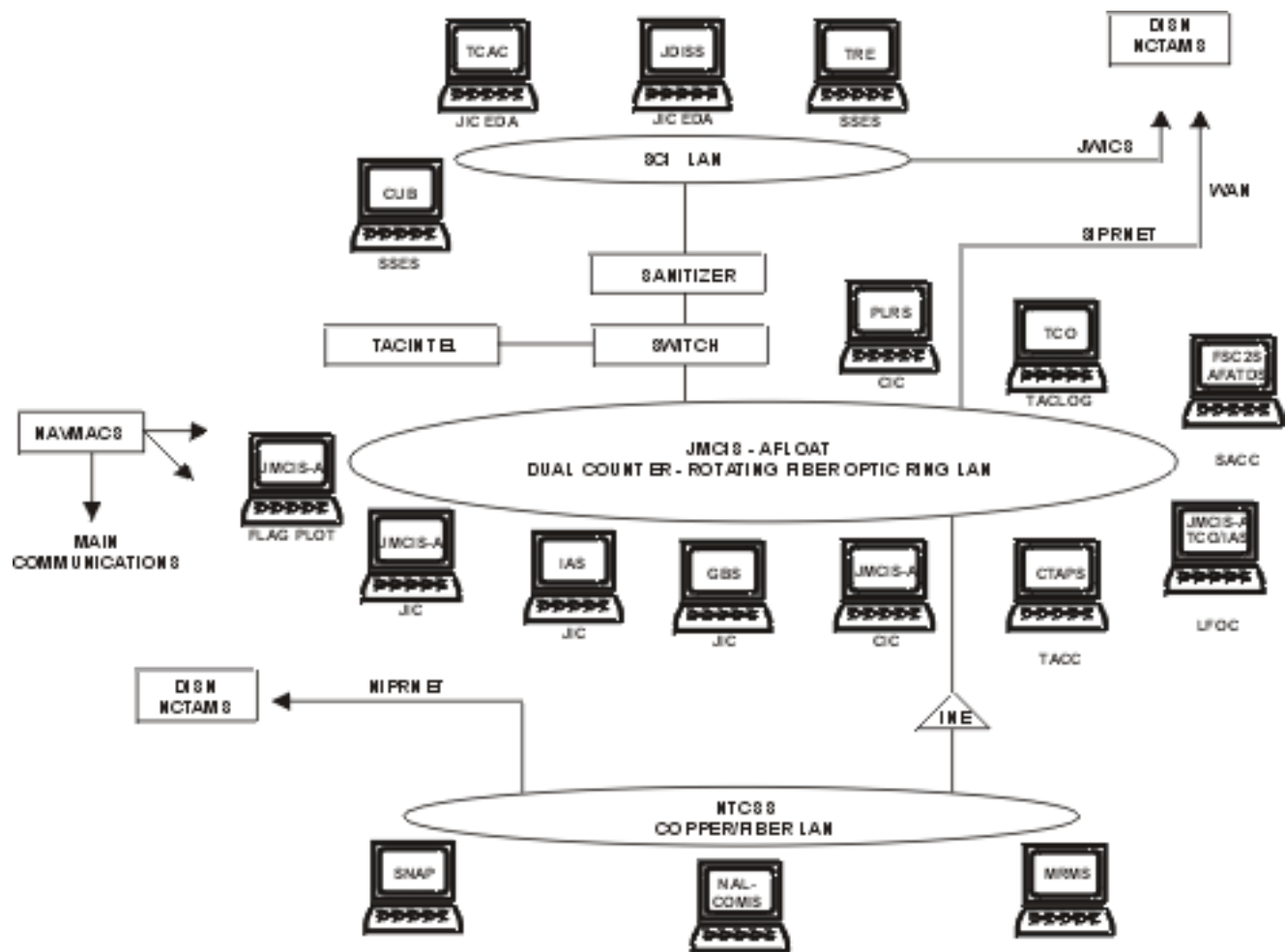


Figure 3-6. Amphibious Ship Information Systems.

Chapter 4

Defense Information Systems Network

The goal of DOD communications architects is a single, integrated, common-user, global communications network. This network, the DISN, will provide support for exchange of voice, data, imagery, and video from strategic to tactical levels, at all echelons, in garrison or when deployed. DOD and the Services are implementing DISN in an evolutionary manner by interfacing and integrating existing communications networks and maximizing commercial services and standards.

Just as GCCS and the DII COE are shaping the future of MAGTF C4I systems, DISN implementation is shaping the Marine Corps tactical communications architecture. For the near term, the communications networks supporting the MAGTF will include the current MAGTF tactical communications networks, the Tri-Services Tactical Communications System (TRI-TAC) switched backbone, SCR, LANs, and special-purpose networks with an interface to DISN for long-haul communications (see chap. 5). However, change is occurring rapidly with the introduction of router-based data communications systems augmenting the switched backbone and providing enhanced connectivity among tactical networks and between tactical networks and DISN.

DISN is the information-transfer segment of the DII. The objective of DISN is the creation of a single, integrated telecommunications infrastructure that can provide end-to-end communications connectivity in support of military operations worldwide. DISN is evolving toward that objective through continuous upgrades to switching and transmission centers around the world and through consolidation and integration of satellite and terrestrial communications networks. DISN currently provides long-haul, common-user, dedicated, secure and nonsecure, voice, data, and video service through a mix of both DOD-dedicated and standard commercial communications services. DISN

provides the communications backbone for other DOD-wide systems including the Secure Voice System, DMS, Defense Data Transport Network nonsecure internet protocol router network (NIPRNET) and SIPRNET, video teleconferencing, and JWICS, as well as separate systems and networks serving the CINCs, Services, and agencies.

4001. Tactical Entry Points

As a first step in DISN implementation, DISA established the Integrated Tactical-Strategic Data Network (ITSDN) to provide an IP router-based data network to support deployed forces. IP router networks are described later in this chapter. Access to ITSDN was provided through SIPRNET and NIPRNET gateways consisting of IP routers and appropriate encryption devices. ITSDN entry points were established at the following locations:

- Ft. Belvoir, VA.
- Wahiawa, HI.
- Northwest, VA.
- Ft. Buckner, Japan.
- Ft. Meade, MD.
- Riyadh, Saudi Arabia.
- Ft. Detrick, MD.
- Landstuhl, Germany.
- Camp Roberts, CA.
- Croughton, United Kingdom.

These ten sites have been upgraded. The four sites listed below have been established to provide 14 DISA standard tactical entry points (STEPS).

- Ft. Bragg, NC.
- Bahrain.
- MacDill AFB, FL.
- Lago Patria, Italy.

Upgrades include installation of the Defense Satellite Communications System (DSCS), the integrated digital network exchange (IDNX), and an interface to the Navy Tactical Network. The STEP sites are also called Defense Communications System entry points, GMF gateways, or DISN gateways. MAGTFs and forward-deployed forces use these STEP sites to access DISN to conduct training, exercises, and operations. When ashore, the MAGTF's primary means to access the STEP sites is through GMF tactical satellite (TACSAT) communications over the DSCS. Shipboard access is provided through the Navy Tactical Network. Five entry points with Navy-unique configurations are located at naval computer and telecommunications area master stations (NCTAMS) to provide both ship-to-shore and ship-to-ship communications. Figure 4-1 depicts a JTF notional architecture with a STEP site and NCTAMS providing the DISN entry.

4002. DISN STEP Services

The services provided to the deployed MAGTF through the DISN STEP include voice, data, and video. Voice services consist of the Defense Switched Network (DSN) and, for secure voice, the Defense Red Switch Network. Data and video services are provided through NIPRNET, SIPRNET, JWICS, and video teleconferencing.

a. DSN

STEP provides one T1 (1.544 Mbps) circuit transcoded to support 48 interswitch trunks to a DSN multifunction switch. These 32 kbps interswitch trunks allow tactical users to place either nonsecure or secure telephone unit-type III (STU-III) calls to a DSN subscriber.

b. Defense Red Switch Network

A single STEP accommodates up to four 56 kbps circuits to the Defense Red Switch Network switch. Each circuit provides two interswitch trunks between the tactical and Defense Red Switch Network switches. These eight interswitch

trunks allow tactical users to place secure red switch calls from the field.

c. NIPRNET

NIPRNET is an information network that is based on IP routers and IDNX smart multiplexers. NIPRNET is designed for sensitive but unclassified information transfer. It supports unclassified networks such as the Marine Corps Data Network and the Tactical Automated Weather Distribution System. Under the ITSDN program, 10 of the 14 STEP sites were configured with NIPRNET routers. MAGTFs use the NIPRNET both aboard ship and ashore to transfer administrative data.

d. SIPRNET

SIPRNET is an information network based on IP routers and IDNX smart multiplexers and designed for exchanging classified information up to and including the secret level. It supports exchanging classified data among GCCS, DMS, CTAPS, TCO, IAS, and other tactical information systems. SIPRNET routers are collocated with NIPRNET routers at 10 STEP sites. MAGTFs use the SIPRNET both aboard ship and ashore to transfer operational data.

e. JWICS

JWICS is an information network based on both IDNX smart multiplexers and IP routers. It is designed for exchange of SCI-level video and data information. It supports the MAGTF's use of INTELINK and other services such as those accessed by using JDISS and TCAC. MAGTFs access JWICS while aboard ship and in operations ashore.

f. Video Teleconferencing

Higher echelons use video teleconferencing with increasing frequency. Within the operating forces, it is used primarily for MAGTF-to-JTF/CINC coordination. Currently, video teleconferencing supports only point-to-point conferencing. In the future, multipoint conferencing will also be supported.

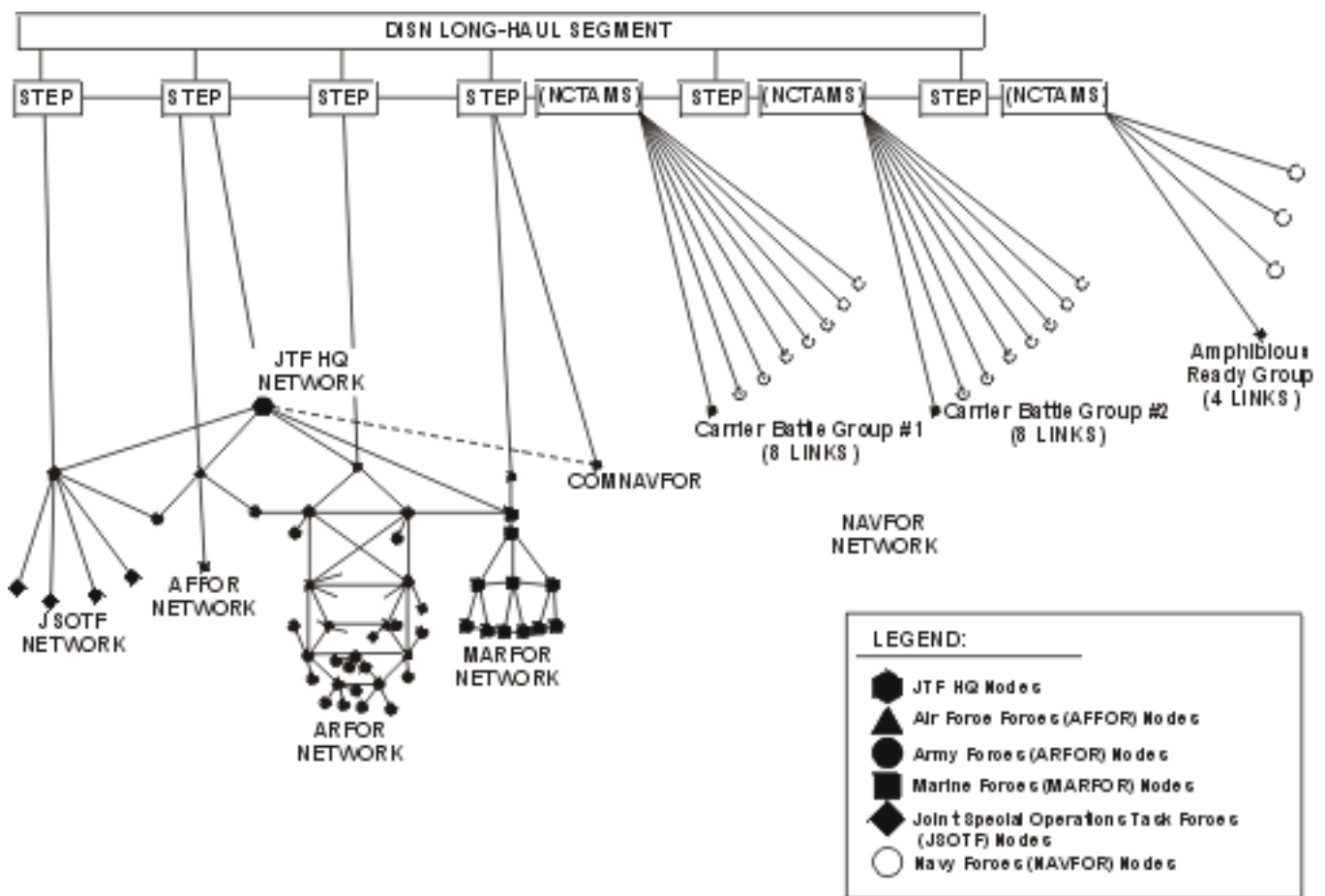


Figure 4-1. JTF Notional Architecture.

4003. STEP Access

The STEP access process is different for the MAGTAF GMF/TRI-TAC terminals than it is for Navy shipboard terminals. The STEP access equipment at the entry points is assigned to either GMF/TRI-TAC or Navy. The GMF/TRI-TAC access equipment is managed by DISA, and the Navy-unique access equipment is managed by the Navy. DISA manages the satellite power and bandwidth for DSCS. DISA also assigns MAGTF (i.e., GMF/TRI-TAC) users particular STEP sites according to priority and equipment/service capabilities.

The various DISA monitoring centers that control NIPRNET and SIPRNET router configurations and programming are listed below. When a circuit is activated and a router-to-router connection is made or attempted, the DISA monitoring center

must be contacted. A previously issued mission directive (described below) references the DISA monitoring center supporting an operation or exercise. The DISA analyst ensures that all routers are configured properly to support the operation/exercise. DISA has the capability to modify routing tables and configurations as required:

- Columbus, OH (NIPRNET Regional Control Center).
- Washington, DC (SIPRNET Regional Control Center).
- Oahu, HI (Pacific).
- Vaihingen, Germany (Europe).

Procedures for GMF/TRI-TAC access to an entry point and satellite are described in the CJCSM 6231 series. Theater-specific access procedures are described in DISA contingency exercise plans.

Theater access procedures for the western hemisphere (including the continental United States [CONUS]) are governed by Contingency Exercise Plan 10-95, for the European theater by Contingency Exercise Plan 1-96, and for the Pacific theater by Contingency Exercise Plan 203-92. Access is initiated with the MAGTF G-6/S-6 request to the theater DISA Contingency Operations Branch and a satellite access request to the Regional Space Support Center, either directly or through the JTF J-6. The request specifies the services required. DISA responds with an SHF/GMF mission directive and a satellite access authorization. The mission directive is a message that identifies entry points and points of contact to establish the access. The priority and purpose of the request, based on the MAGTF mission, should determine the speed at which entry point access is granted.

The mission directive also provides IP addressing, router information, port and channel assignment, and coordination points of contact for each data network. For additional information on ITSDN, see the IP Addressing Plan and the CJCSM 6231 series documents. The communication battalion's data network officer and system planning and engineering officer maintain copies of these and other DISA documents.

4004. Changes to DISN STEP Sites

Change is continuous in the DISN evolution. DISN sites and the tactical users must remain adaptable to obtain the more robust and flexible services provided by the upgraded IDNX backbone. The joint communications support element (JCSE) that provides CINC/JTF support committed funding for IDNX upgrades to meet the goal communications architecture. IDNX provides link bandwidth management that allocates circuits as needed. It allows for a virtual network with automatic routing and rerouting. It also sets the stage for an evolutionary transition to the use of asynchronous transfer mode (ATM). As these changes take place, MAGTFs will require similar equipment to take advantage of the more robust global

network structure. For additional information, see CJCSM 6231.07A.

4005. USMC Network Operations Center

Assistance from outside the MAGTF is available from the USMC Network Operations Center. The USMC Network Operations Center provides technical support for MAGTF and supporting establishment WAN managers and acts as the primary point of contact for all Marine Corps operational issues in the area of communications networking. The USMC Network Operations Center acts as the Marine Corps Service-level representative to DISA, other DOD agencies, and commercial vendors concerning network operational issues and products.

The USMC Network Operations Center operates 24 hours a day, 7 days a week supporting the Marine Corps communications infrastructure as a whole. It performs the following tasks:

- Reports/resolves problems.
- Distributes networking software.
- Provides network infrastructure components inventory.
- Serves as the Marine Corps network registration authority as assigned by the DISA network information center.
- Provides centralized management and funding of Marine Corps telecommunications services that traverse DISN, NIPRNET, SIPRNET, LAN-WAN exchange, and IBM Systems Network Architecture networks.
- Serves as Service representative to DISA.
- Coordinates Marine Corps and other Service/agency telecommunications requirements.
- Provides technical assistance teams to requesting units.
- Maintains 16 permanently assigned NIPRNET and 16 permanently assigned SIPRNET Class C addresses for deployed MEU(SOC)s.

Chapter 5

MAGTF Tactical Communications Network

The MAGTF tactical communications network supports information exchange requirements—voice, data, video, and imagery—both internal and external to the MAGTF. For external long-haul communications, the tactical communications net-

work interfaces to DISN. The MAGTF tactical communications network must also interface with the tactical communications networks of the other Services.

Section I

Overview

This overview is designed to give all Marines who use tactical communications an understanding of the capabilities and limitations of these networks. This understanding, in turn, will assist in the effective employment of these networks to conduct operations and accomplish assigned missions.

5101. Architecture

The tactical communications network is composed of numerous subnetworks that interface with one another in varying degrees. These subnetworks themselves are usually referred to as networks. Figure 5-1 depicts the four types of subnetworks—SCR, local area networks, SBB, and special purpose systems. Each is described in sections II–V.

The Marine Corps tactical communications architecture is rapidly evolving to meet the information transfer requirements of the MAGTF and to take advantage of new technology. Changes in the architecture are also driven by the requirement to interface with DISN and to be interoperable with the other Services.

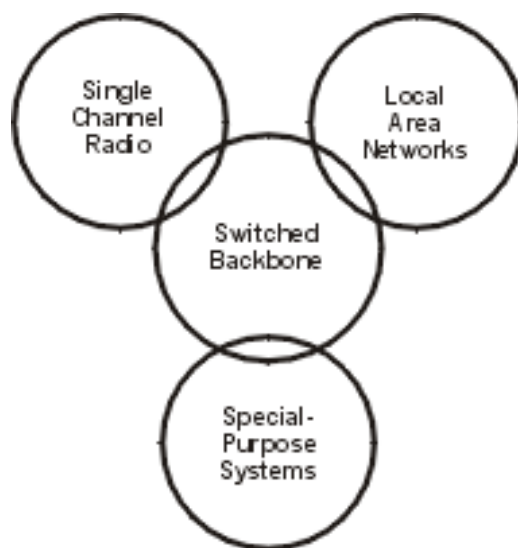


Figure 5-1. MAGTF Tactical Communications Network.

5102. Challenges

The rapid pace of change provides the CIS community with both challenges and opportunities. Perhaps the most critical challenge is to provide maneuver battalions with adequate data communications capability. The ability to provide the

shared situational awareness so critical to the successful execution of any operation depends on meeting this challenge and others. The fundamental requirement remains unchanged—to provide the MAGTF with a reliable, secure, fast, and flexible communications network.

The design of the actual communications architecture to support a MAGTF is based on the nature of the operation, the commander's (JTF, ATF, MAGTF) intent, the concept of operations, and the composition and task-organization of the MAGTF as well as that of attached and support-

ing forces. In the early stages of an operation, SCR usually provides the principal means of communications. As the operation evolves, LANs and SBB networks are established to meet the information transfer requirements of command and control at higher echelons. Maneuver battalions continue to depend on SCR throughout the operation with limited radio interface extensions to the SBB. Special-purpose systems provide dedicated communications support for certain functions, such as position location and navigation and air defense.

Section II

Single Channel Radio

SCR is the principal means of communications support for maneuver units. SCR communications equipment is easy to operate, and networks are easily established, rapidly reconfigured, and, most importantly, easily maintained on the move. SCR provides secure voice communication and supports limited data information exchange. SCR in the VHF and UHF bands is normally limited to line of sight. In the HF band, SCR can support long-range communications, albeit at the expense of mobility. SCR SATCOM provide mobility, flexibility, and ease of operation with unlimited range. Limitations of SCR include susceptibility to enemy electronic warfare; cosite, footprint, terrain, and atmospheric interference; the requirement for close coordination and detailed planning; a need for common timing, frequency, and equipment; and limited spectrum availability. The latter is particularly critical in the case of SATCOM.

MAGTF SCR equipment is fielded in many configurations and includes hand-held, manpack, vehicle-mounted, ground-mounted, and sheltered radios. These radios operate in simplex and half-duplex modes. The most widely employed tactical radios provide integrated COMSEC and jam resistance through frequency hopping. Tactical SCRs operate in the three military radio frequency bands shown in table 5-1. Characteristics of each category are discussed in paragraphs 5201 through 5203.

SCR is used primarily for secure voice communications. However, SCR can also transmit and receive data by using terminal devices such as the Digital Message System (previously called and more commonly known as the Digital Communications Terminal [DCT]) and the TCIM. The DCT and the TCIM are described in this section because of their critical role in enabling data communications at the tactical level over SCRs. (See app. A.)

Table 5-1. Ground SCRs.

Frequency Band	MAGTF SCR Equipment Used	Operating Frequency Range	Typical Application
HF	AN/PRC-104 AN/GRC-193 AN/MRC-138	2–29.999 MHz	Radio line of sight and beyond/long range
VHF	AN/PRC-68 AN/PRC-77 VRC-12 family SINCGARS family	30–88 MHz	Radio line of sight and relay/retransmission
	AN/PRC-113 AN/VRC-83	116–150 MHz	Critical line of sight (ground to air)
UHF	AN/PRC-113 AN/VRC-83 AN/GRC-171	225–400 MHz	Critical line of sight (ground to air)
	AN/PSC-3 AN/PSC-5		SATCOM footprint

5201. HF Radio

HF radio equipment is capable of both long- and short-range secure voice and data communications. Data communications capability is typically limited to rates of 2.4 kbps. Data transmission requires modems specifically designed for operation in this band of the radio spectrum. MAGTF HF radio equipment includes the AN/PRC-104 manpack, the vehicle-mounted AN/MRC-138, the AN/GRC-193, and the AN/TSC-120 with automatic link establishment capability.

The primary advantage of using HF radio is its capability to provide long-range, OTH communication. Successful data communication over the HF range depends on several factors: equipment siting, proper equipment grounding, types of antennas used, tactical employment of radio equipment, path assessment and analysis, and frequency planning and assignment. When commercial data terminal equipment (DTE) is used, users employing HF radio equipment need to be aware of radio interference and potential shock hazards that can easily affect unprotected DTE. Whenever possible, HF radio equipment should be remotored from DTE.

The primary limiting factors when using HF radios are frequency allocation/management and bandwidth availability. Frequency allocation/management is concerned with frequency, time of day, time of year, and location. The ability to reflect HF radio waves off the ionosphere to a distant location is in a constant state of flux because of activity in the ionosphere.

The sun's radiation causes disturbances in the ionosphere, with most changes taking place in what is known as the F-layer. Sunrise and sunset can be the most difficult times for HF communications. The F-layer splits into two separate layers around sunrise and recombines into one layer around sunset. These splits affect transmission distances as the area "skipped over" increases and decreases. At times, solar storms can completely eliminate all HF communications.

HF transmission paths must be constantly monitored to achieve a dependable HF link. HF radio data communications capabilities are limited by the bandwidth that is imposed by legal constraints and the physics of the spectrum. The bandwidth available in the HF spectrum limits the channel bandwidth, which in turn limits data throughput.

5202. VHF Radio

The primary MAGTF VHF radio is the single channel ground and airborne radio system (SINCGARS). SINCGARS is a family of lightweight combat radios that serves as the primary means of communications for command and control and fire support on the battlefield. SINCGARS is the standard VHF-frequency modulated (FM) tactical radio for the Marine Corps, replacing the AN/PRC-77 and the AN/VRC-12 family. The system provides high security against threat EW by using frequency hopping with integrated COMSEC. It is capable of voice and data transmission (up to 16 kbps under optimum conditions and over limited distances) over the VHF-FM frequency range of 30–87.975 MHz.

There are seven different SINCGARS configurations available, depending on the requirements of the user. These configurations include the manpack, typically used in infantry operations, and vehicle-mounted variants. The radio provides voice communications ranges of up to 8 km for the manpack and 35 km for vehicular configurations. SINCGARS is capable of remote operation by using the analog AN/GRA-39B radio remote control, the digital HYX-57 wire-line adapter, or the digital C-11561(C)/U remote control unit (RCU).

a. Systems Improvement Program

The SINCGARS radio has undergone a systems improvement program (SIP). This radio is referred to as the SINCGARS SIP. The primary improvements relate to the data transmission capabilities of the system. A forward error correction appliqué, was implemented in the receiver/transmitter and a new packet data mode was created to better support packet networks. An improved channel access protocol was added which

optimizes data throughput performance while minimizing impact on voice communications on the same SINCGARS channel.

The SINCGARS SIP radio is also available in a downsized version, the result of an advanced systems improvement program (ASIP). This radio is referred to as the SINCGARS ASIP. This radio will retain all the functionality of the full size SIP radio in half the size at a total weight of 7.6 pounds (including the battery). The radio is interchangeable with previous SINCGARS versions, including the capability to be mounted in older vehicular adapter assemblies. A new feature of the SINCGARS ASIP provides a retransmission capability while operating in the packet data mode and will also employ a new fast channel access protocol for improved operations in shared voice/data nets.

The AN/ARC-210 multipurpose radio supports single-channel air-to-air, air-to-ground, and ground-to-air communications in tactical Navy/Marine Corps fixed- and rotary-wing aircraft. It has the capability to transmit and receive VHF-FM, VHF-amplitude modulation (AM), and UHF. It is compatible with SINCGARS in the frequency hopping mode, as well as with HAVE QUICK and HAVE QUICK II frequency hopping UHF radios, and it can accept 25 preset single-channel frequencies. The AN/ARC-210 requires a TSEC/KY-58 encryption device to encrypt transmissions and decrypt received signals.

b. Employment Considerations

Attention to operator maintenance of the radio equipment, antennas, cable assemblies, and equipment grounding, as well as site planning and selection, is essential to reliable communications. Frequency separation, radio antenna separation, remote keying when using COMSEC, and power output are significant employment factors.

When operating with some Navy ships, SINCGARS may be limited to the single-channel mode. When SINCGARS is employed in the frequency hopping mode, the following operating factors need to be taken into account: hopset (frequency segment allocation), time of day (system

clock), antenna placement (cosite interference is more of a concern than in the single-channel operating mode), and power setting. SINCGARS radios configured for different hopsets that dial into the same numbered net will not be able to communicate. MCRP 6-22A, *TALK II-SINCGARS: MSCP for the Single Channel Ground and Airborne Radio System*, provides detailed information on the employment of SINCGARS.

VHF SCR is the primary communications system for combat and combat support units while on the move. The predominant mode of operation is secure voice. However, use of VHF radio for data communication will increase with the fielding of tactical information systems at the battalion level and below.

Small, handheld VHF radios are used at the small-unit level in the MAGTF. These radios are often commercial items that lack compatibility with SINCGARS and do not have integrated COMSEC. Their use should be governed accordingly.

c. Environmental Limitations

The primary limiting factors when using VHF radios are range and frequency availability. VHF radios can provide reliable communication for ranges of up to 10 miles, depending on the equipment operating constraints and the operating environment. When employing radios that operate in the VHF spectrum, consideration must be given to unit location. Most circuits are limited to radio line of sight, known as 4/3 earth curvature. VHF radio signals essentially follow the curvature of the earth to a distance that is approximately 1/3 greater than the distance to the horizon. Foliage interferes with VHF signals and may reduce normal operating ranges to significantly less than 10 miles.

5203. UHF Radio

Military UHF radio equipment operates in the 116-150 MHz upper VHF frequency range and the 225-400 MHz military UHF radio spectrum. MAGTF UHF radio sets (AN/PRC-113, AN/VRC-83, and AN/GRC-171) are capable of data

communication at 16 kbps under optimal conditions. MAGTF ground and airborne UHF radios incorporate the HAVE QUICK electronic counter-counter measures capability and operate in single-channel and frequency hopping modes. The HAVE QUICK UHF radio is capable of remote operation by using the AN/GRA-39B or HYX-57.

The UHF radios are used for forward air control ground-to-air communication. Line of sight between radios is critical for reliable communication. Significant range differences are encountered between UHF radios employed for ground-to-air and ground-to-ground communications. Greater range is achieved when employed from ground to air because of the increased line of sight. When employed in the frequency hopping mode, the following operating factors must be understood for proper operation: hopset, time of day, antenna placement, and power setting.

The primary limiting factor when using UHF radios is range (critical line of sight). Critical line of sight can be described as “what you see is what you get.” As long as the radio’s antenna has optical line of sight to another radio’s antenna, the two will be able to transmit and receive. For this reason, UHF radios are primarily used in air-to-ground communications.

5204. EPLRS

EPLRS shares many characteristics with PLRS, but provides a significant increase in data communications capability over PLRS. Various data rates supporting a variety of broadcast and point-to-point modes are currently available. Thus, EPLRS will provide a dedicated data communications capability between regiment and battalion tactical data networks (TDNs) within the ground combat element, when fielded in FY-00. This network will also be extended to lower echelons throughout the MAGTF. EPLRS can also serve as a source for automated friendly position location information (PLI) and navigation information in a hybrid community with PLRS, though data throughput is reduced. A NCS-E(D) is currently required to establish an EPLRS communications network, however, efforts are underway to contin-

ue to reduce its size. Ultimately a “laptop” communications network initialization capability is envisioned, concurrent with increased functionality within the radio set itself. (See fig. 5-2.)

5205. UHF-TACSAT

The AN/PSC-5 Enhanced Manpack UHF terminal employs both narrowband (5 kHz) and wideband (25 kHz) channels supporting 2.4 and 16 kbps data transfer rates, respectively. UHF-TACSAT radios are employed for long-range communication. Multiple-access schemes can operate either with fixed channel assignments to the various users or with channels being assigned in varying fashion according to demand. The latter is called demand assigned multiple access (DAMA). With demand assignment the user makes a channel request, and, after a brief time lag, a channel is allocated. The DAMA scheme of operation is employed on UHF-TACSAT to share available channels more efficiently. The radio systems are compatible with the KY-57 (wideband mode only), the KY-99 and ANDVT (narrowband mode only), and the KG-84C (wideband or narrowband) COMSEC equipment. This radio equipment is also capable of remote operations by using the AN/GRA-39B (narrowband mode) or HYX-57 (wideband mode).

a. Employment Considerations

Because of its limited availability, the MAGTF employs TACSAT primarily to support critical, long-range communications requirements (e.g., communications support for deep reconnaissance operations or connectivity to the tactical echelon of a MEU(SOC) when deployed ashore). The AN/PSC-5 is the primary DAMA-capable TACSAT radio available to the MAGTF.

TACSAT limitations include the competition for available frequency resources and channel time on the satellite. If only narrowband channels are available, channel data rates are limited to 2,400 bps. Channel congestion, noise, and network saturation will affect the information flow on satellite channels and will require a significant reduction in the data transmission rates to sustain data communication. Transmit power selection can be

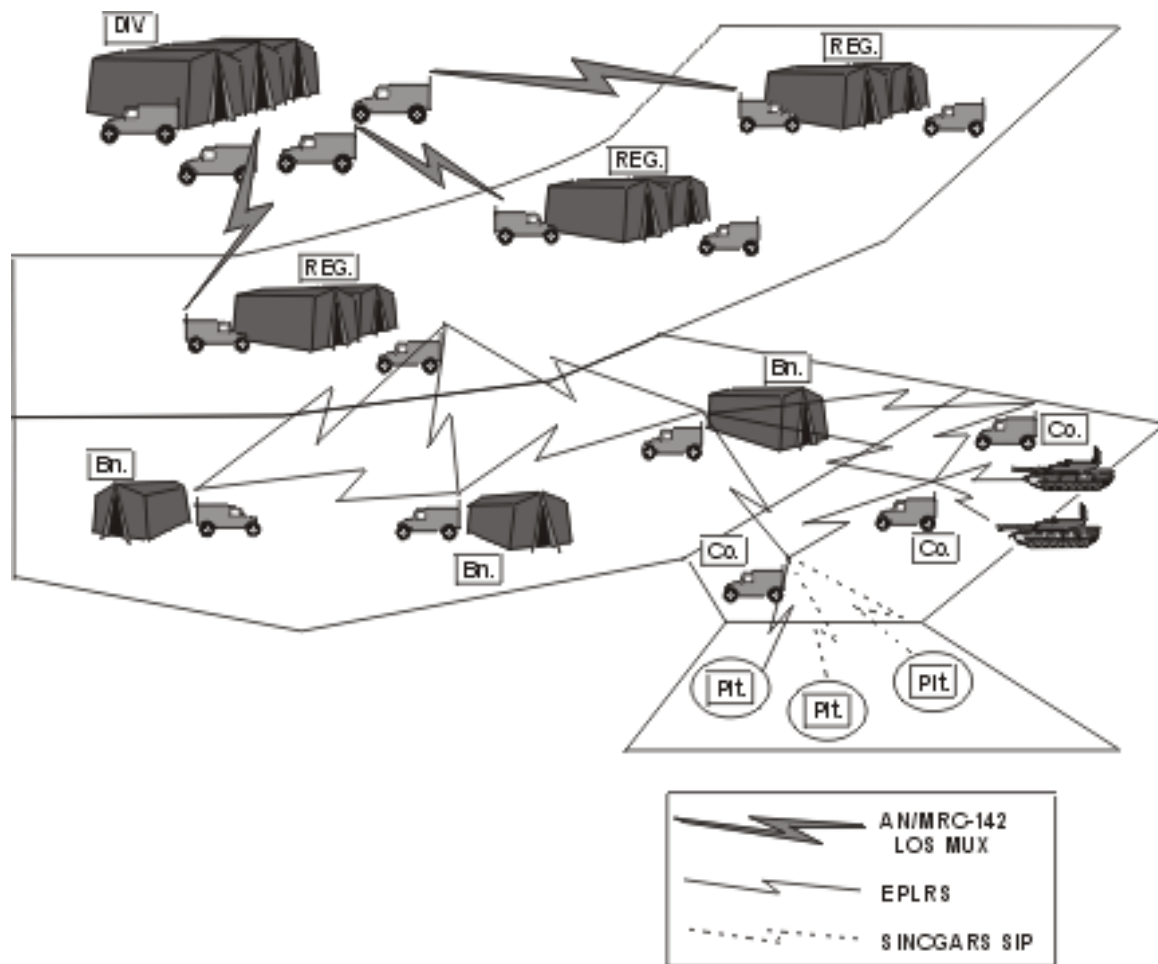


Figure 5-2. EPLRS COE.

critical. Sometimes increasing the transmit power can decrease net effectiveness. Larger directional antennas provide increased signal gain, which increases the transmitted signal power. Antennas for these systems are lightweight and fragile and, therefore, require constant maintenance and inspection for proper operation.

b. Environmental Limitations

The primary environmental limitations on TAC-SAT radios are signal propagation delay, location on the earth, terrain masking, and weather effects. Timing between DTE can be a critical factor in SATCOM because the satellite, acting as a relay between radios, is about 25,000 miles away. There is approximately a one-fourth second propagation delay between sending and receiving sta-

tions. This delay can interfere with systems that automatically retransmit if an acknowledgment is not received after a very short timeout period.

As unit location changes, the “look angle” (angle above the horizon) to the satellite can affect net reliability. The orbit of a satellite allows it to cover a certain footprint on the earth. Satellites in equatorial orbit can cover large portions of the earth both north and south of the equator, but as the user moves closer to the earth’s poles, the TACSAT terminal may exceed the satellite footprint. This will cause intermittent or lost communications. Terrain can also have this effect by interfering with the satellite and TACSAT terminal line of sight. Thunderstorms, heavy snowstorms, and hail also affect satellite transmissions

both by damage to antennas and effect on the electromagnetic environment.

5206. Commercial International Maritime Satellite

INMARSAT is a commercial L-band UHF system originally designed to support merchant vessels and cruise ships with telephonic communications. It is used by the military on a surge basis to satisfy demands that military satellites cannot meet. Significant restrictions on the use of INMARSAT are its cost and lack of security. It is a pay-as-you-go service that costs \$5–\$8 per minute. Because of these high usage costs, INMARSAT should be used only when other tactical communications cannot support the operation effectively. The advantage to INMARSAT is its availability with minimum advance coordination, although it could potentially become saturated during a major crisis. Planning for use of INMARSAT requires coordination and approval from the MAGTF G-6/S-6 and arrangements for connection and payment of bills.

To access the INMARSAT satellite constellation, the Marine Corps can employ any one of a variety of manpack and mobile systems. These terminals communicate via satellite with a shore station that provides the connection to the global terrestrial network. INMARSAT radio employment considerations and environmental limitations are much the same as those for military TACSAT.

5207. Data Communications

Although data communications will never completely replace voice communications on the battlefield, for certain functions it is essential. Examples are functions such as reconnaissance, where transmit time must be minimized, and fire support, where rapid, accurate fire support request processing is critical. Furthermore, as tactical information systems such as TCO are fielded to lower echelons, the requirement for data communications will expand dramatically.

a. DCT (AN/PSC-2)

The DCT is a rugged, lightweight, microprocessor-controlled, handheld message processor. It provides Marine users at all echelons with point-to-point and netted data communications and is compatible with most MAGTF radio, wire, and encryption equipment. It supports data transfer up to 2.4 kbps in the analog frequency shift keying (FSK) mode and, depending on the transmission media, up to 16 kbps in the digital baseband mode. The DCT allows the operator to enter and read data in both free text and fixed or variable message formats (VMFs). VMF is the tactical message standard adopted by DOD for ground forces. All of the Services have agreed to use this standard.

DCT communications protocols and modulation techniques are interoperable with those of the TCIM used at MAGTF CPs. DCTs are used by the Army for both fire support and intelligence applications, and a DCT interface is available onboard the LHD-1 class of amphibious ships.

Forward air controllers, forward observers, Stinger teams, and reconnaissance teams are the primary users of the DCT. Employment of this device enables one-time entry of the data, incorporating burst transmission for reduced on-air time. The DCT supports standard message formats for accurate, consistent, and machine-readable information exchange. Effective DCT employment requires training and a commander's willingness to take the time required to set up data communications nets rather than relying strictly on voice communications. Proper DCT operation results in a key command and control capability—the ability to exchange data at the tactical level.

b. Data Automated Communications Terminal

The DACT is a small, tactical computer and communications terminal which gives users the capability to receive, process, and transmit various messages, to include text and symbology, used by tactical data systems. The DACT will effectively replace the DCT when it achieves full operational capability in FY 03, but will provide much greater functionality below battalion levels. This will

include an embedded GPS receiver, the ability to share a common picture of the battlespace, automated data exchange, and MAGTF C4I network connectivity. The DACT will be transportable by foot mobile Marines and mounted in tactical or armored vehicles.

c. TCIM

TCIM provides interfaces between MAGTF information systems and communications systems. It is used to connect standalone terminals with SCR nets and to pool radio resources at operation centers for more efficient use of equipment and frequencies. TCIM provides operations centers with the ability to receive and transmit a set of standard tactical netted messages processed by the DCT and other tactical information systems. As an MCHS communications processor for MAGTF information systems, TCIM provides the data network interface for MAGTF command, control, communications, computers, and intelligence information systems at various facilities, agencies, centers, and individual locations. It supports data exchange over radio, wire, and TRI-TAC SBB networks.

Three types of TCIMs are available with various software versions that support a wide variety of communications protocols. The three types include an internal PC card, an external set of cards mounted in a small metal box, and a PC card variant that requires a compatible PCMCIA card slot in the computer. TCIM interfaces to the computer by using the open systems standard small computer system interface (SCSI) and the serial RS-232C (7-wire) interface. Programmable wire-line, multipurpose, and radio port interfaces are provided on the network side of TCIM.

Communications protocols supported include TACFIRE, combat net radio, battery computer system, gun direction unit, Marine tactical systems (MTS), MIL-STD-188-220A variable message format (VMF), commercial, Army mobile subscriber equipment (MSE) tactical packet switch network, and EPLRS X.25 packet switch protocols. This network interface device allows data exchange with Marine and other Service elements using compatible protocols. The DCT can exchange data with information systems that use TCIM.

Section III

Local Area Networks

MAGTF LANs are data communications networks designed to support information exchange, collaboration, and resource sharing in a particular agency, facility, center, cell, or geographic location. Because of the limited distances involved, network signal protocols can be designed to support high data throughput—up to 100 Mbps, although 10 Mbps is more common. These LANs include terminal equipment connected to a transmission medium such as wire or fiber-optic cable. The terminal equipment exchanges data by using a protocol that is compatible with the medium. MAGTF LANs use both copper wire and fiber-optic cable of various types configured to meet the tactical information exchange requirements of the command. Specific LAN access methods, technologies, protocols, and equipment are employed in a topology that connects the commands' information systems and services. This section addresses the basic types of LAN media, topologies (physical and logical layout or design), and access methods in use by the MAGTF.

This section describes the LAN environment and some of its many implementations. MAGTF LAN implementations will change with time because of continuous change in the technology and resulting commercial products. DOD acquisition directives require the Services to implement COTS and GOTS products where they are feasible and cost-effective. As these very products compete in the commercial marketplace, it is incumbent on CIS personnel to remain aware of these changes to be able to employ the most effective LAN cables, topologies, and access media in coordination with Marine Corps- and DII-specified standards.

5301. LAN Media

LAN media include copper-based coaxial and twisted-pair cable used within local facilities, such as a regimental-level COC and fiber-optic cable used for higher-speed backbone connections

connecting multiple facilities in a large HQ complex. Fiber-optic backbone LANs are also used aboard Navy ships in conjunction with copper-based coaxial and twisted-pair LANs within an operational workspace such as the LFOC.

a. Unshielded Twisted-Pair Cable

Unshielded twisted-pair cable is increasingly the commercial LAN cable of choice. Unshielded twisted-pair cable is economically priced, widely available, and relatively easy to install, operate, and maintain, making it particularly attractive for MAGTF employment. The MAGTF requires that LANs be easily and quickly set up and dismantled to support rapid and frequent displacements on the battlefield. Less specialized installation equipment and training are major considerations driving Marine Corps use of unshielded twisted-pair cable. Twisted-pair cable comes in several gauges (more commonly referred to as categories in LAN terminology), based on the number of twists per foot, with categories 3, 4, and 5 being the most desirable for LAN connectivity. Smaller gauges, used for subscriber telephone line installations, should not be used for data transmission. Local networking using unshielded twisted-pair cables requires hubs or concentrators to provide retransmission of signals and assist in maintenance. Unshielded twisted-pair LANs are not reliable in environments with high electromagnetic interference (EMI). In these environments, wire cables must be shielded, routed around interference sources, or replaced with fiber-optic cable.

b. Shielded Cable

Shielded LAN cable options include shielded twisted-pair and coaxial cable. Shielded twisted-pair cable has many of the advantages of unshielded twisted-pair cable, but costs more in return for supporting greater segment lengths and a relatively limited shielding capability. Coaxial cable is available in both thick and thin diameters. Thick coaxial cable allows greater noise immunity and longer cable runs than does thin coaxial

cable. Shielded LAN cables are used by MAGTFs only when necessary to achieve greater distance without repeaters and as a lower-cost alternative to fiber-optic cable.

c. Fiber-Optic Cable

Fiber-optic cable provides high speed over long distances with immunity to electromagnetic interference. Greater levels of security are possible with this cable because it is very difficult to tap. Glass fiber-optic cable is many times more transparent than its plastic counterpart, and, therefore, it is the primary type used for LAN applications. This cable is available in single- and multimode fiber based on its light conducting or propagation characteristics. Single-mode fiber is much thinner than multimode fiber and provides higher transmission throughput at distances much greater than a few miles.

Single-mode fiber uses lasers as an intense light source and is the most expensive to install. Multimode fiber uses dispersed light signals; this reduces its transmission throughput and its effective cable length to distances of less than a mile. Multimode fiber uses the much more cost-effective and weaker light source provided by light-emitting diodes. Therefore, if a MAGTF fiber-optic LAN backbone capability made of interconnecting, 1-km or less segments is suitable, the cheaper multimode fiber capability would be acceptable. The MAGTF Fiber-Optic Cable System currently in the supply inventory can be used for the tactical data network (TDN) backbone, with appropriate connector modifications.

Fiber-optic cables require two fibers to allow two-way (full duplex) communications. MAGTF fiber-optic cable is bundled with two fibers in a single cable, but commercial fiber-optic cable is also available as single-fiber cable. The glass fibers are surrounded by a reflecting wrap, a plastic coating, a layer of tough material such as Kevlar, and an outermost jacket for protection. Two disadvantages of fiber-optic cable are its low tolerance for bends in the cable and poorly constructed or maintained connectors. Light transmission tolerances are critical for these cables to operate properly.

d. Shipboard Media

In an effort to improve information access and resource sharing, upgrades to shipboard LANs are constantly underway. As ships are cycled through service life extension, they receive the latest networking technology. However, it may be several years between overhauls, leaving much of the fleet with older, less responsive networking equipment. Many older shipboard LANs were installed with thick coaxial cable, while newer shipboard LANs use both fiber-optic backbones and twisted-pair or thin-wire coaxial cable extensions from hubs to workstation terminals. Embarked MAGTFs do not use the older thick-cable LANs because they cannot adequately support multiple additional users. In these cases, embarked MAGTFs are often authorized to install their own temporary, unshielded twisted-pair or thin-wire coaxial LANs.

e. Media Selection

The higher cost and increased complexity of installation and maintenance of coaxial cable and fiber-optic LANs is sometimes outweighed by their capability to span greater distances without repeaters and, in the case of fiber-optic cable, much greater throughput capacity. This is particularly true in the choice of a backbone media to support a larger HQ such as the MEF or an MSC. On the other hand, at the cells and centers of the larger HQ and at tactical echelons, regiment and below, media selection will be driven by ease of installation and operation, and data throughput requirements will not be as great. In most cases, this will lead to a choice of unshielded twisted-pair cable.

5302. LAN Topologies

LAN topologies are described by both their physical configuration (bus, star, or ring) and their logical implementation. The most common physical topologies in use by the MAGTF are the bus and star, with the star becoming more prevalent. Shipboard physical topologies include bus, star, and ring. The fiber-optic backbone on most ships is arranged as a ring, with star-configured LANs connected to the ring. Logical topologies describe the way the LAN is viewed by the media access

method used. For example, Ethernet uses both the bus and star physical topologies while implementing a bus-type logical topology.

a. Bus Topology

The bus physical topology requires the least amount of cable and is the simplest of the three. Terminal devices are attached using drop lines to points along the cable where a tap is used to penetrate the cable, or, alternatively, quick disconnect hardware is used at planned breaks in the cable. Signals transmitted on the bus propagate to every point on the bus in a broadcast fashion. Any device connected to the bus can communicate with any and all other devices on the bus over this broadcast medium. The ends of the bus require terminating devices with an impedance that matches that of the cable (typically 50 ohms for baseband coaxial cable). Without this matched termination, reflected signals would interfere with intended transmissions. (See fig. 5-3.)

The bus topology is usually used with contention-based media access methods such as Ethernet. This topology is also frequently used as a backbone transmission path for other topologies, which allows multiple specifications and access methods in a more complex network. Buses use specifications that restrict overall cable length. Length restrictions are necessary to ensure that timing measurements associated with signal propagation and collisions on the cable can be used to manage the network.

The bus topology may be desirable for smaller LANs at tactical echelons where its simplicity and ease of installation may outweigh its disadvantages.

Installation and reconfigurations tend to be simpler with a single cable. Less equipment, wiring, and infrastructure are required for the bus compared to other topologies; therefore, installation and operating costs are likely to be lower. Multiport transceivers, bus attachment devices that allow multiple terminal drops from one connection to the bus, transform the bus topology to a star. The flexibility of being able to reroute the terminal drops without moving the bus is a further advantage of this topology.

The shared nature of the bus topology is the cause of its disadvantages. Any disconnected or broken cable will disable the entire LAN. Minimum distances between connected terminal devices are imposed to reduce adjacent terminal signal reflections and to allow sufficient time for collision detection schemes to operate properly. Bus cables are restricted in length through imposed specifications to ensure that signal propagation delay never exceeds the time needed to send the shortest allowable message over the LAN. The thin-wire LAN cable specification 10Base2, for example, indicates with the number "2" that the maximum cable length is 200 meters. Actual cable lengths are somewhat less than the approximate numbers used in the abbreviated specifications.

b. Star Topology

The star topology is characterized by multiple terminal devices homed or connected to a central hub or server. Unlike the bus, the star topology continues to operate for all other connected devices if one of its terminals or a cable to one of its terminals malfunctions. This topology, although more complex than the bus, can be more efficient

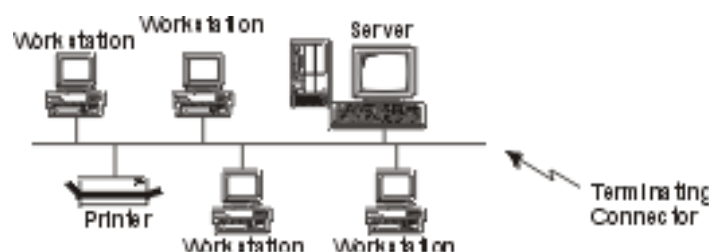


Figure 5-3. Bus Topology.

and is the most widely used LAN topology in commercial and MAGTF applications. (See fig. 5-4.)

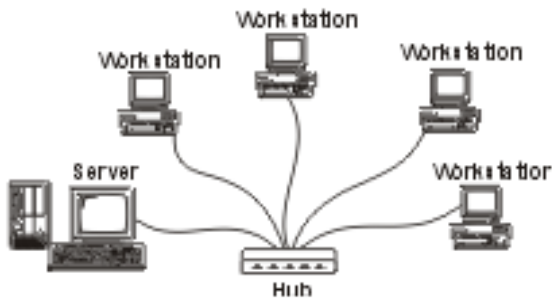


Figure 5-4. Star Topology.

Advantages of the star topology include excellent diagnostic, control, and management capabilities. Priority schemes can be employed as a way of managing the various workstations and other terminal devices on the LAN. Because all terminal devices connect to the hub, all lines are easily monitored and controlled. Reconfiguration is also much easier to manage at this centralized location. (See fig. 5-5.)

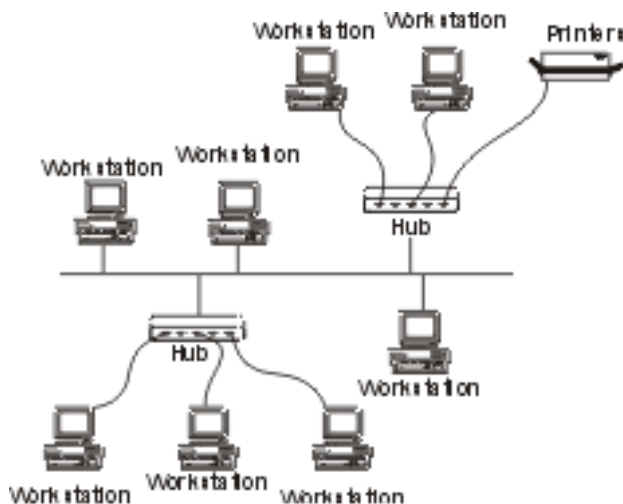


Figure 5-5. Combined Bus/Star Topology.

The star topology's disadvantages center around its centralized hub, also called a concentrator. The hub is a common point of failure for all of the

connected terminals. If the hub loses power or has a failure in its circuitry, the entire LAN may be shut down. If the failed hub is attached to a backbone bus when it fails, the entire bus could also be disrupted. The additional wiring for terminal connections and the hubs themselves adds to the cost of this type of topology. Despite the higher cost, the added flexibility and convenience of the star topology make it the topology most often used in the MAGTF.

c. Ring Topology

In the ring topology, all terminals are connected to one another to form a circular ring with communications possible in either direction. Typically, one of the terminals acts as the manager or monitor in the network. The monitor is responsible for generating and passing the token that controls other terminal users' access to the ring. Only the holder of the token is allowed to transmit on the LAN. Once completed, that user sends the token to the next user on the ring. The ring is generally associated with token-passing access methods such as token ring or fiber distributed data interface (FDDI). (See fig. 5-6.)



Figure 5-6. Ring Topology.

The implementation of this topology is most often combined with the star topology using hubs on the ring as multiple access units for terminal connections. This access method reduces failures and interruptions that would occur if terminals were connected in a series of point-to-point connections to form the ring. (See fig. 5-7 on page 5-14.)

The hubs are left in place, reducing the chance of failure introduced by constant interruption caused

by user connections and disconnections. One bad connection on any part of the ring, however, can bring the entire LAN down. The hubs are part of the ring, and their failure to maintain the ring connection can cause the backbone LAN to fail. Dual rings are used to overcome this single point of failure. Usually, one ring is the primary ring, while the other (secondary ring) is a backup that is used if the primary ring fails. As with the star topology, the ring topology includes excellent diagnostic, control, and management capabilities. This topology is prevalent aboard ship.

5303. Access Methods

LAN access methods define the processes, procedures, and standards for the various types of media and topologies. The Institute of Electrical and Electronic Engineers (IEEE) 802 series specifies standards for LAN media access methods. The IEEE 802 series includes Carrier Sense Multiple Access with Collision Detection (CSMA/CD or 802.3), token bus (802.4), and token ring (802.5) access methods. These access methods, originally used with copper wire at data rates of 1 - 16 Mbps are now also used with fiber-optic cable and can be used at 100-Mbps data rates. The FDDI and corresponding copper distributed data interface

access methods are specifically developed for 100 Mbps fiber-optic and copper LANs. Ethernet, a specific implementation of the 802.3 access method, is the most widely used LAN standard in the world. It is also, not surprisingly, the most widely used LAN access method in the MAGTF and aboard ship. Ethernet is used with multiple media types and topologies. Ethernet standards are specified for twisted-pair, coaxial, and fiber-optic LAN media. Table 5-2 shows approximate maximum data rates, cable types, approximate maximum cable segment lengths, topologies, and the number of segments and nodes per segment for each Ethernet specification.

The FDDI access method specifies a 100 Mbps, token-passing, dual-ring LAN that uses the fiber-optic transmission medium. It defines the physical layer and media-access portion of the link layer. FDDI access is similar in many ways to Token Ring access. Both use the ring topology, token passing, and redundant features such as dual rings.

FDDI is defined by specifications for media access control, physical layer protocols and medium, and station management. FDDI, however, uses the same upper sublayer of the datalink layer that Ethernet uses, making it compatible with

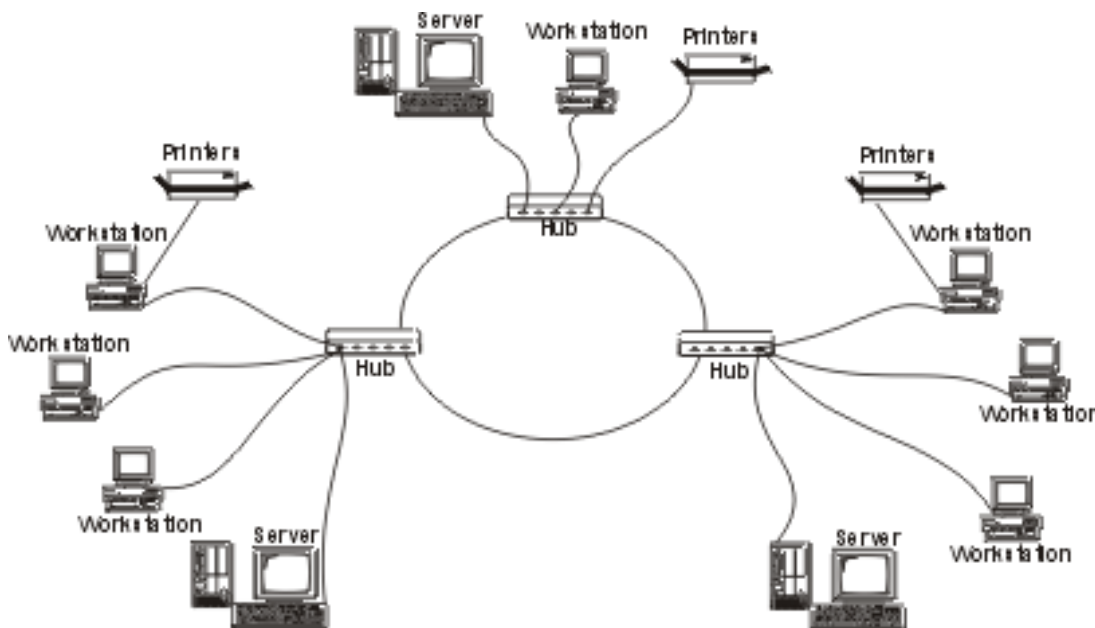


Figure 5-7. Combined Ring/Star Topology.

Table 5-2. Ethernet Standards and Specifications.

Specification Name ¹	Maximum Data Rate	Cable Type	Maximum Length of One Cable Segment (meters)	Bus Type Topology	Number of Segments/Nodes per Segment
10BaseT	10 Mbps	Twisted-pair Category: 3, 4, 5	100	Star	Depends on hub ports
10Base2	10 Mbps	Coaxial (thin)	200.00	Linear ²	3/30
10Base5	10 Mbps	Coaxial (thick)	500	Linear ²	5/250
10BaseFL	10 Mbps	Fiber-optic	4000.00	Star	
100BaseFX/TX	10 Mbps 100 Mbps	Twisted-pair (Category 5)	150	Star	Depends on hub ports
¹ Specifications are all baseband, with the first number indicating the maximum data rate in Mbps and the last letter/number indicating the cable type or the unrepeatable cable length. ² Impedance matching terminations at ends of cables required.					

Ethernet at its higher throughput. Media access control defines the medium access method, which includes frame format, token handling, addressing, the algorithm for calculating a cyclic redundancy check value for error detection, and error recovery mechanisms. The physical layer protocol defines data coding procedures, clocking, framing, and other requirements. The physical layer medium defines the transmission medium, which includes the fiber-optic link, power levels, bit-error rates, optical components, and connectors. Station management involves the FDDI station and ring configurations and ring control features such as station insertion and removal, initialization, fault isolation and recovery, scheduling, and statistics collection.

FDDI employs two traffic types, synchronous and asynchronous, to provide real-time allocation of network bandwidth. A portion of the total 100 Mbps bandwidth can be allocated solely for synchronous traffic, while asynchronous traffic uses the remainder. Stations with the need for continuous transmission capability, such as simultaneous voice, data, and video information applications, use synchronous traffic. The remaining bandwidth is used by asynchronous traffic users who have much lower throughput requirements. Station management functions of FDDI include a distributed bidding scheme to allocate FDDI bandwidth based on an eight-level priority scheme. These capabilities for flexible bandwidth allocation are useful in the larger MEF HQ to ensure effective use of limited bandwidth.

Section IV

Switched Backbone

The MAGTF switched backbone (SBB) comprises the switching, routing, and wideband transmission systems that provide the high-capacity communications backbone for the MAGTF tactical communications network as well as connectivity with the DISN. It is the tactical equivalent of commercial local and long-distance networks and, in some situations, interfaces with and uses those commercial networks. The SBB uses an evolution of older and newer equipment and technology. The evolution drives changes in systems and organizations, revisions in procedures, and requirements for additional training.

The SBB, like the MAGTF itself, is tailored and has the flexibility to adapt to support the unfolding tactical situation and overall scheme of maneuver. The SBB is planned, designed, installed, operated, and maintained by CIS personnel under the cognizance of the G-6/S-6 and leadership of communications unit commanders. Planning, redesign, and adaptation are continuous as SBB equipment and personnel arrive in theater and the MAGTF transitions to operations ashore. Larger HQ, rear areas, expeditionary airfields, and C2 facilities are the principal subscribers to the SBB. Maneuver battalions cannot afford the restrictions on mobility imposed by the SBB and normally link to it through an SCR interface.

The switches, IP routers, and wideband MCR systems that form the MAGTF SBB are described in this chapter. Computers play a key role in the operation, maintenance, and control of this SBB. Computer-controlled communication links and switching enable efficient, flexible use of limited resources. Computerized switches and routers are used to route voice, data, and video information at various points or nodes in the network. They include devices such as circuit switches to route telephone calls and data, message switches to route organizational message traffic, packet switches for efficient data transmission, and routers to interface with IP router networks for data

communications. Wideband MCRs, both satellite and terrestrial, provide the internodal communications for the MAGTF communications network and the connectivity to the DISN entry points. (See app. E.)

5401. Tri-Services Tactical System

The TRI-TAC family of equipment, developed in the 1970s under a joint program of the Marine Corps, Air Force, and Army and fielded in the mid-1980s, provides the major components of the MAGTF SBB. This equipment was developed to provide interoperable, secure, and deployable voice and data digital switching and transmission systems for tactical forces operating in a joint environment. The design took into consideration the realities of tactical communications in remote locations. Tactical transmission links are constrained by high bit-error rates and limited bandwidth, and TRI-TAC systems are designed to operate in this environment.

TRI-TAC systems provide a high degree of security but are complicated, expensive, difficult to operate, and use a very different set of communications standards than the commercial networks and the DSN. For voice digitization, TRI-TAC systems employ continuously variable slope delta (CVSD) modulation to conserve transmission bandwidth, while the DSN and commercial networks use pulse-code modulation and adaptive differential pulse-code modulation. These differences require modulation conversions at interface points between the TRI-TAC and DSN or commercial networks. Multiple modulation signal conversions eventually lead to errors that disrupt circuits.

TRI-TAC systems use conditioned diphasic signaling, which allows longer wire-line transmission without repeaters than commercial baseband

signaling techniques and permits timing to be embedded in every circuit. This type of signal also provides a much more efficient use of bandwidth than commercial baseband signaling. Again, however, the different signaling techniques drive a requirement for conversion to interface with DSN and commercial networks.

The TRI-TAC family of TACSAT and terrestrial microwave MCR communications and switching systems equipment is currently in use by three Services and the joint community—the Army at echelons above corps level, the Marine Corps at regiment/group and higher echelons, the Air Force when deployed, and the JCSE to support JTFs. The employment of TRI-TAC systems began before Desert Shield/Desert Storm and provided, with some growing pains, an unprecedented degree of communications interoperability between the Army, Marine Corps, and Air Force.

GMF tactical SATCOM systems include DSCS satellites that provide the required relay and compatible ground terminal systems. Terminal systems include the AN/TSC-85 and AN/TSC-93, which are fielded in the MAGTF in limited numbers. The Army also uses these terminals, while the Air Force uses interoperable versions—the AN/TSC-100 and AN/TSC-94 terminals. Marine component and MEF HQ are routinely augmented with Air Force and Army GMF SATCOM terminals for training and contingencies under memorandums of understanding (MOUs) with the Army and Air Force.

There are five different TRI-TAC circuit switches and two versions of the TRI-TAC message switch. Each switch has its own software that must be frequently tested and certified to ensure that it will interoperate with the other switches in the network. The Marine Corps and the Air Force employ the TRI-TAC-developed AN/TTC-42 and SB-3865 unit-level circuit switches (ULCSs). The large, high-capacity AN/TTC-39 circuit switch and AN/TYC-39 message switch are also TRI-TAC switches but are not part of the Marine Corps inventory. However, these two switches are available, with support personnel, under the same

Army and Air Force MOUs used to obtain GMF SATCOM augmentation. TRI-TAC switches use deterministic routing like the DSN and commercial networks, while the Army's AN/TTC-39D and MSE switches use an incompatible flood-search routing scheme.

5402. Switches

Switches provide the means to route traffic through a network of transmission media supporting many commands, units, and individual Marines. Switching may be manual (operator assisted) or automatic, and it may connect local subscribers, such as those in a MEF main COC, or perform WAN functions, such as sending traffic over satellite links. There are basically three types of switches: circuit, message, and packet.

Circuit switches generally support telephone traffic; message switches process formatted messages for storage and delivery; and packet switches process data into packets for transmission over multiple links and then reassemble the packets at the other end. Although the Marine Corps developed a packet switch under the TRI-TAC program, it was never fielded, and the Marine Corps achieves a packet switching capability through the use of IP routers as discussed below. The Army, in contrast, employs an X.25 packet switching protocol in conjunction with their MSE equipment to establish a tactical packet network. Exchanging data between the MAGTF SBB and the Army tactical packet network will be a requirement in most joint operations and will be discussed later.

a. Circuit Switches

Circuit switches provide an electrical circuit on demand between calling and called parties. The circuit is reserved for exclusive use of the parties until the connection is terminated. The tactical telephone system operates by means of circuit switching. Circuit switches are used to switch voice, data, and multimedia traffic. Traffic may originate from either data capable terminal devices, secure telephones, nonsecure telephones, or IP routers used to route LAN traffic within the MAGTF and over WANs.

(1) AN/TTC-42 and SB-3865. The MAGTF uses two ULCSs: the AN/TTC-42 and the SB-3865. AN/TTC-42 switches can provide service to 280 combined digital/analog loops/trunks. An SB-3865 switch can provide service to 64 combined digital/analog loops/trunks in a single configuration, and two or three SB-3865s may be stacked to serve 90 combined digital/analog loops/trunks at a single site. Because routing of calls is deterministic, a tactical telephone directory must be maintained.

(2) Digital Transmission Groups. DTGs are used to interconnect switches and are usually encrypted to provide traffic flow security. DTGs may be transported by using GMF SATCOM, line of sight microwave radio, tropospheric-scatter (troposcatter) microwave radio, coaxial cable, and fiber-optic cable.

(3) Interface to the DSN. TRI-TAC switches interface to the DSN through STEPs. STEPs are configured to provide the interface between the tactical and DSN systems. Because a direct digital CVSD-to-pulse-code modulation conversion has not yet been implemented in the STEPs, the interface between the tactical communications system and the DSN consists of converting tactical CVSD-modulated circuits to analog form, interfacing the analog signal with the DSN, then digitizing the signal into 64 kbps pulse-code modulation or 32 kbps adaptive differential pulse-code modulation format for further transmission within the DSN.

(4) Interface to MSE. TRI-TAC switches interface to MSE switches via designated area codes known as “area code gateways.” These area codes are used within MSE as the means of interfacing between the MSE flood-search network and external deterministic networks such as DSN and TRI-TAC.

(5) North Atlantic Treaty Organization and Commercial Interfaces. TRI-TAC AN/TTC-39 family switches contain hardware and software features that allow them to interface with NATO members’ switches in accordance with Standardization Agreement (STANAG) 5040. STANAGs 4206 through 4213 provide specifications for

standard digital interfaces between NATO tactical communications systems. The AN/TTC-42 and SB-3865 switches do not implement NATO interfaces and rely on AN/TTC-39 family switches to provide NATO access if it is required.

(6) Security. The TRI-TAC system employs digital subscriber voice terminals (DSVTs) to provide end-to-end encryption for classified conversations and uses link encryption of interswitch digital transmission groups to conceal the number of calls made over the link and the telephone numbers called (i.e., traffic flow security). Although not designed as part of the TRI-TAC system, STU-III terminals are used to provide secure access to subscribers in the DSN. DSVT, digital nonsecure voice terminal (DNVT), and analog telephones cannot be used to place secure calls into the DSN because they are cryptographically incompatible with the STU-III terminals. DSVT, DNVT, and analog telephones can place nonsecure calls to STU-III terminals connected to the DSN or commercial networks. A STU-III multimedia terminal can be used for interfaces with DNVT devices for interface to the TRI-TAC communications network.

(7) Access. Telephones (DSVT, DNVT, and multimedia terminal), TCIMs, radio-wire integration devices, remote multiplexer combiners (RMCs), and electrical/optical converters are used to gain access to circuit switches (see table 5-3). Telephone lines may be multiplexed/combined by RMC devices before entering the circuit switch. Many of the tactical telephones are both data and voice capable. The TCIM provides a computer-to-radio or computer-to-circuit switch interface capability. Radio-wire integration devices provide manual, remote access to the SBB from SCR systems. RMCs extend the service area of a local circuit switch by providing wire-line access to a limited number of subscribers who do not possess or have direct access to a switch. Electrical/optical converters allow for connection of fiber-optic cable between switches and other parts of the communications network

(8) Analog Equipment. Some older analog circuit switches and telephones remain in the inventory. These devices can interface to the SBB, but

not in a secure digital mode. Consequently, their primary utility lies in providing local telephone service within a single CP or HQ. These analog devices are described in TM-2000-15/2B, *Principal Technical Characteristics of U.S. Marine Corps Communication-Electronic Equipment*.

Table 5-3. MAGTF Telephones.

Analog	TA-312 TA-838 TA-938 STU-III ¹
Digital	TA-954 DNVT TA-1042 DNVT ¹ TSEC/KY-68/78 DSVT ¹ Multimedia terminal (STU-III) ¹
¹ Data capable	

More information on circuit switching can be obtained from TRI-TAC manuals and in CJCSM 6231.02, *Joint Voice Communications Systems* and CJCSM 6231.03A. The older tactical telephones are described in TM 2000-15/2B.

b. Message Switches

Message switches ensure delivery of complete messages to a distant location or multiple locations when circuits to that location become available. If all circuits are busy, the originating message center or intermediate message switches store the message and automatically transmit it to the proper addressee as soon as a circuit is free. This form of switching is referred to as “store and forward.”

Message switches are primarily used by the MAGTF at the MEF CE and MSC levels. The AN/MS-63A is used to support both general service (GENSER) and SCI message switching. The designations for these two message switch uses are the Tactical Communications Center (TCC) for the GENSER message switch and the Special Security Communications Central (SSCC) for

SCI. As mentioned earlier, the AN/TYC-39 message switch is available from the Army to augment the message switching capability of the MEF.

c. Packet Switches

Transmission of complete messages is an inefficient use of data communications networks. Packet switches break messages into data packets that are individually addressed and entered into the network. The packets are forwarded to the addressee over a number of different links or circuit paths between packet switches based on circuit availability. At the receiving end of the circuit, the packets are reassembled into the original message, which is then passed to the receiving terminal. The MAGTF does not use packet switches. However, the MAGTF circuit switches may have to interface with the Army’s MSE. MSE employs a tactical packet network overlay to accomplish packet switching over its circuit switches. MSE supports division units in the Army. Special interface equipment and protocols are required to accomplish this interface.

d. Switch Network

MAGTF switches are used primarily at the regiment level and higher echelons at the main and rear area operations centers. MAGTF switches and associated subscriber devices are listed in table 5-4 on page 5-20.

Switches are now available in increasingly small packages such as circuit cards. This enables the use of these switches within or as embedded components of other systems such as digital TECHCON equipment and TDN servers and gateways. Routers, described next, are also migrating to enclosures such as those described above and perform similar functions to those of switches. Figure 5-8 (on page 5-20) shows circuit switch connectivity for a MEF in a JTF. CJCSM 6231.02 and CJCSM 6231.03A provide more detailed information about tactical circuit and message switch descriptions and use.

Table 5-4. MAGTF Switches.

Switch	Location Used	Interface Devices	Terminal Devices	Type
AN-TTC-42	MEF/MSC	TCIM IP routers	STU-III	Circuit
SB-3865	MEF/MSC Regiment/group Artillery regiment/ battalion		DNVT DSVT	
AN/MS-63A AN/TYC-39	MEF/ACE/division MEF/MARFOR		Message servers	Message

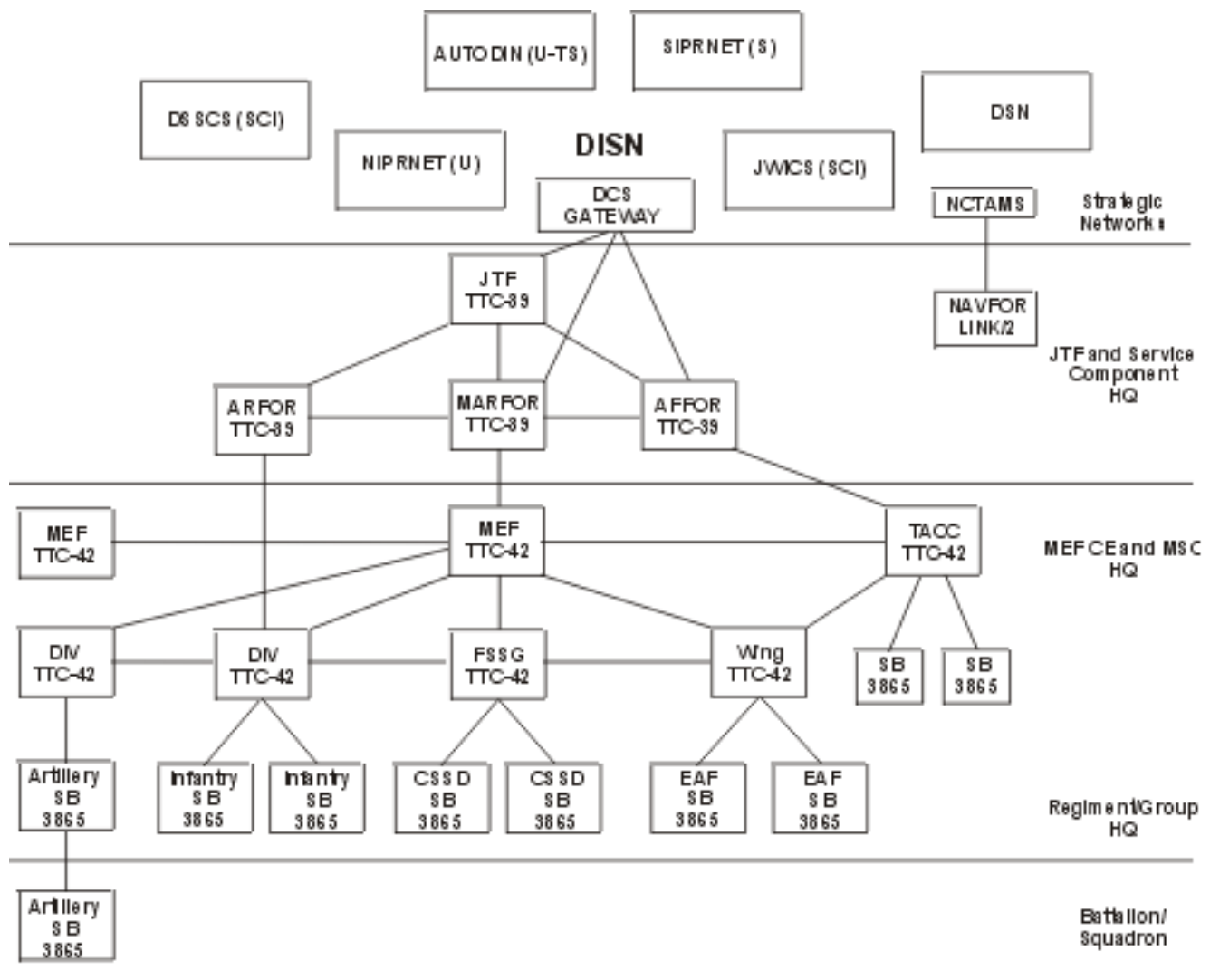


Figure 5-8. Circuit Switch Network.

5403. Global Block Numbering Plan

Effective 1 June 1995 the Global Block Numbering Plan (GBNP) was implemented by all tactical circuit switches and switchboards in the Department of Defense. The GBNP does not violate the deterministic use of 3/4 or 4/3 numbering plans. The plan was designed to be compatible with numbering plans previously used for joint operations and the Military Services. Incorporation of the plan should be done during the normal cycle when contingency, exercise, and operations plans are updated.

The basis for the GBNP is fourfold: (1) to incorporate all Services into a joint network, (2) to identify a unique, Service-managed block of unit and subscriber numbers, (3) to simplify network management (DISN/Commercial) routing into a global network, and (4) to identify data bases and subnetworks within the block of numbers. The GBNP must be implemented with the circuit switch routing - task execution plan (CSR-TEP) to preclude NNXX contention between flood search and deterministic subscribers and to allow deterministic switches to route into the flood search network.

HQMC (C4I) is the policy and oversight authority for the USMC's GBNP and Preaffiliation List (PAL) management. PAL management will be centralized at the USMC and major command level (COMMARFORPAC, COMMARFORLANT, and COMMARFORRES). As of June 1998, MARCORSYSCOM is designated the USMC PAL Manager; MCTSSA will be the action organization. The USMC PAL Manager will—

- Coordinate, distribute and maintain the USMC PAL assignments as delineated by the Global PAL Manager (U.S. Army).
- Serve as the Marine Corps' primary Point of Contact for the Global PAL Manager (U.S. Army).
- Coordinate and assist the major commands in establishing PAL and PAL sublists and maintain this information in a centralized database.

- Recommend any policy requirements that facilitate the management and assignment of PALs To HQMC (C4I) on an as needed basis.
- Coordinate with COMMARLOGBASES on equipment related issues.
- Coordinate with MCCDC to ensure that USMC PAL assignments are incorporated into the appropriate doctrinal publications.

5404. IP Routers

The modern battlefield demands that the SBB provide efficient support for data communications. Although circuit switches and message switches can support data communications, packet switching is far more efficient. The Marine Corps initially planned to establish a packet switching network using a packet switch developed under the TRI-TAC program. However, the Army chose to implement an X.25-based packet switching network as an overlay on its MSE network. This Army decision and other factors led the Marine Corps to abandon the TRI-TAC packet switch, known as the unit-level message switch. Instead, the Marine Corps has developed a packet switching capability through the use of commercial IP routers. This placed the Marine Corps in an excellent position in terms of connectivity to DISN because DISA has transitioned the strategic DISN Defense Data Network (DDN) from a network based on X.25 packet switching to one based on IP routers.

The Marine Corps uses commercially available IP routers to automatically route traffic to and from local or remote subscriber LANs, over the SBB, and to and from the DISN. These IP routers form a data communications overlay on the SBB and serve as gateways to the IP router networks of the other Services, the JTF, and DISN. MAGTF computers are configured to operate by using their unique IP address(es). These computers implement the TCP to handle end-to-end delivery of messages on IP router networks.

IP routers route data packets containing data in multiple formats throughout the DISN IP router networks: JWICS, SIPRNET and NIPRNET.

Inline network encryptors and COMSEC encryption equipment are used to provide packet-level and transmission security of the IP router networks. IP routers provide the gateways between the LAN and the SBB. IP routers use exterior protocols along with interior protocols to handle IP-addressed packets, determine paths to destinations or other routers, and manage the IP packet flow through their nodes. CJCSM 6231.07A, chapter VIII, provides information about router protocols and IP addressing used by the DISN.

a. Notional Air-Deployable Data Communications Package

A typical air-deployable, router-based data communications package to support the MAGTF CE includes the equipment in table 5-5.

Table 5-5. Notional Air-Deployable Data Communications Package.

Nomenclature	Quantity
Heavy HMMWV with shelter	2
Banyan server suite	4
Laptop (router)	2
Desktop suite (net management)	3
CISCO 4000 router	3
LAN repeater	3
Uninterruptible power supply (UPS)	7
Channel service unit (CSU)/ data service unit (DSU) modems	4
Asynchronous modems	2
KG-84C	8
KYK-13/data transfer device (DTD)	2
KOI-18	2

This equipment, with appropriate CIS personnel and transmission equipment, provides the following capabilities:

- NIPRNET, SIPRNET, and JWICS WAN access to a gateway/higher HQ.
- NIPRNET, SIPRNET, and JWICS WAN access for seven MSCs/adjacent units.
- NIPRNET, SIPRNET, and JWICS LAN access for 50–200 end users.
- TDS network management.
- IP router network management.

b. Notional MEF Data Communications Package

A typical router-based data communications package to support the MEF CE includes the equipment in table 5-6.

Table 5-6. MEF CE Data Communications Package.

Nomenclature	Quantity
5-ton truck with shelter	1
Banyan server suite	8
Laptop (router)	2
Desktop suite (net management)	5
CISCO 7000 router	3
CSU/DSU modems	4
Asynchronous modems	2
LAN repeater	8
UPS	11
KG-84C	20
KYK-13/DTD	2
KOI-18	2

This equipment, with appropriate CIS personnel and transmission equipment, provides the following capabilities:

- NIPRNET, SIPRNET, and JWICS WAN access to a gateway/higher HQ.
- NIPRNET, SIPRNET, and JWICS WAN access for seven MSCs/adjacent units.
- NIPRNET, SIPRNET, and JWICS LAN access for 50–200 end users.
- TDS network management.
- IP router network management.

- JTF enabler module.

c. Contingency Data Network Suites

MCTSSA has available, on request, contingency data network suites capable of supporting NIPRNET and SIPRNET WAN access. The contingency data network suite is a standard data network package for MAGTF use until the TDN gateway is fielded. Each contingency data network suite has been designed to support encrypted WAN connectivity to distant CPs and a LAN of up to 48 hosts operating at the same classification level. The contingency data network suite is composed of two CE packages and six remote site packages that differ in size and the number of serial data connections available. Table 5-7 lists the contingency data network suite equipment. The KIV-7 is compatible with the KG-84A/C, but is capable of much higher data rates when interfaced with another KIV-7. The UNIX workstation is capable of supporting a DNS and network management software. The contingency data network suite can be requested from MCTSSA via the MEF G-6.

Table 5-7. Contingency Data Network Suite Equipment.

Item	Quantity
CE Package (x 2)	
CISCO 4500 router	1
KIV-7 encryption device	4
LAN hubs	2
2000VA UPS	1
UNIX workstation	1
Printer (LaserJet)	1
Remote Site Package (x 6)	
CISCO 2514 router	1
KIV-7 encryption device	2

d. TDN

Although the TDN had not been fielded as of the writing of this publication, the operating forces are already using COTS hardware and software to establish tactical data communications networks

and to interface with DISN. TDN will have an initial operational capability in FY 00.

The TDN system augments the existing MAGTF communications infrastructure. It provides the commander with an integrated data network and forms the data communications backbone for MAGTF TDSs. It will replace the interim data communications package with an expeditionary, highly mobile suite of equipment that uses the latest router technology.

The TDN system has two configurations: the TDN gateway and the TDN server. The TDN gateway is deployed at the MEF and MSC levels and provides access to the NIPRNET, the SIPRNET, and other Services' tactical packet switch networks. The TDN gateway consists of an air-conditioned/heated, heavy HMMWV-mounted shelter equipped with the major components listed in table 5-8.

Table 5-8. TDN Gateway Components.

Item	Quantity
MCHS processors	4
Monitors	2
Smart multiplexer IDNX-20	1
Router-multiprotocol Minimum: 8 serial ports 2 802.3 ports 1 asynchronous port	2
Repeater (7-port)	6
TCIM and TCIM power supply	4
KIV-7 encryption device	16
Wire-line adapters	16
UPS	6
SNMP adapter	4
Fiber-optic modems	2
KY-68 DSVT	6
MMT with DNVt appliqué	4
Patch panels EIA 530 Loop	4 2
In-line network encryptor	1

The TDN server is deployed at the MEF, MSCs, and units down to the battalion/squadron level. The TDN server is transported in three transit cases. It includes the equipment shown in figure 5-9. TDN gateways and servers provide the capability to share files, perform electronic message handling, and provide transparent routing of messages through the LAN, circuit switch, MCR, and SCR subnetworks.

e. Future Direction

For more efficient MAGTF interfaces to the DISN, IP routers and smart multiplexers are increasingly replacing the older and less expeditionary switching system equipment. For example, IDNX smart multiplexers are being included at SIPRNET and NIPRNET (DISN) entry points, and the implementation of similar equipment by the MAGTF will enable more efficient and flexible use of available bandwidth. Figure 5-10 shows the many connectivity options available with smart multiplexers.

CJCSM 6231.02 and 6231.03A provide more detailed information about switches, routers, and joint communications networks.

5405. Multichannel Radios

MCR provides the communications links for the SBB. It permits multiple users to access a single communications path. MCR equipment includes terrestrial line of sight, troposcatter, TACSAT, and HF radios, all with associated multiplexers, modems, cabling, and antennas. MCR provides worldwide connectivity through links to the NIPRNET, SIPRNET, and JWICS networks of the DISN as well as the links for long-distance communications within the theater and within the MAGTF. MCR provides reliable, flexible, and high-capacity links for both voice and data communications. Its primary disadvantages are complexity and a lack of mobility. An MCR network requires more time to set up and more expertise to operate and maintain than an SCR network, and it

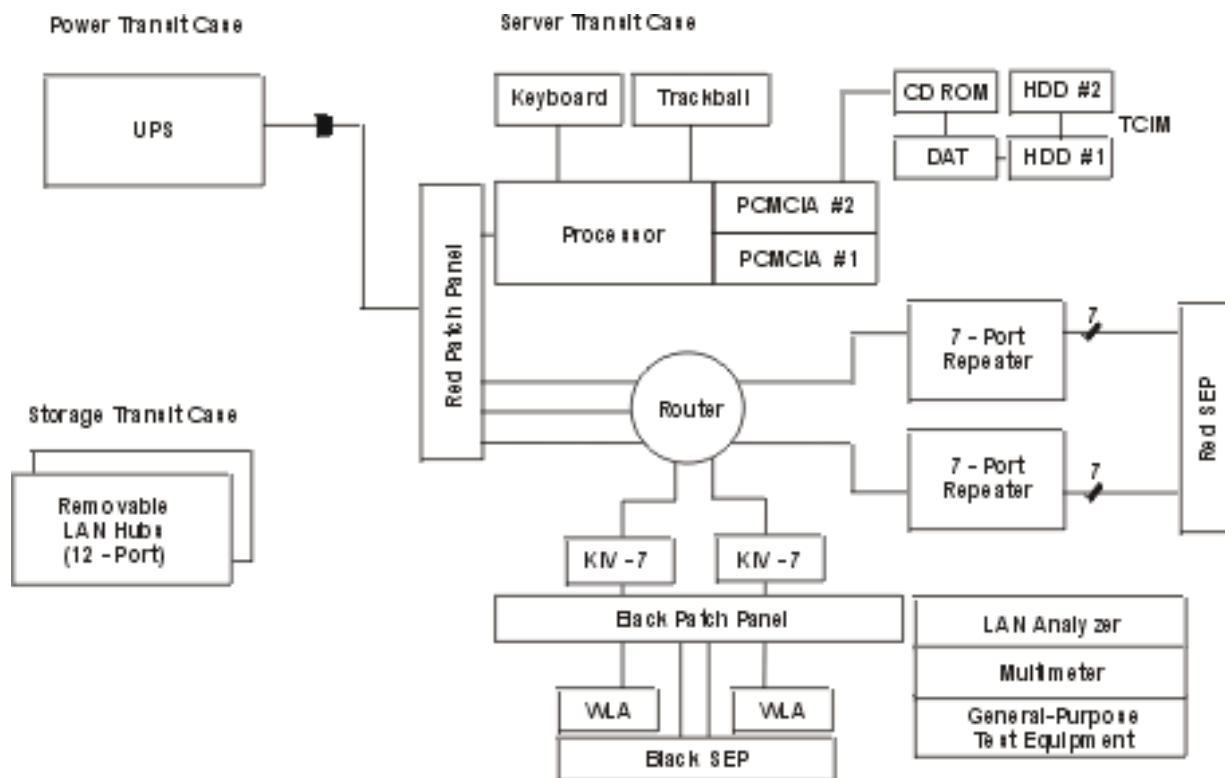


Figure 5-9. TDN Server Components.

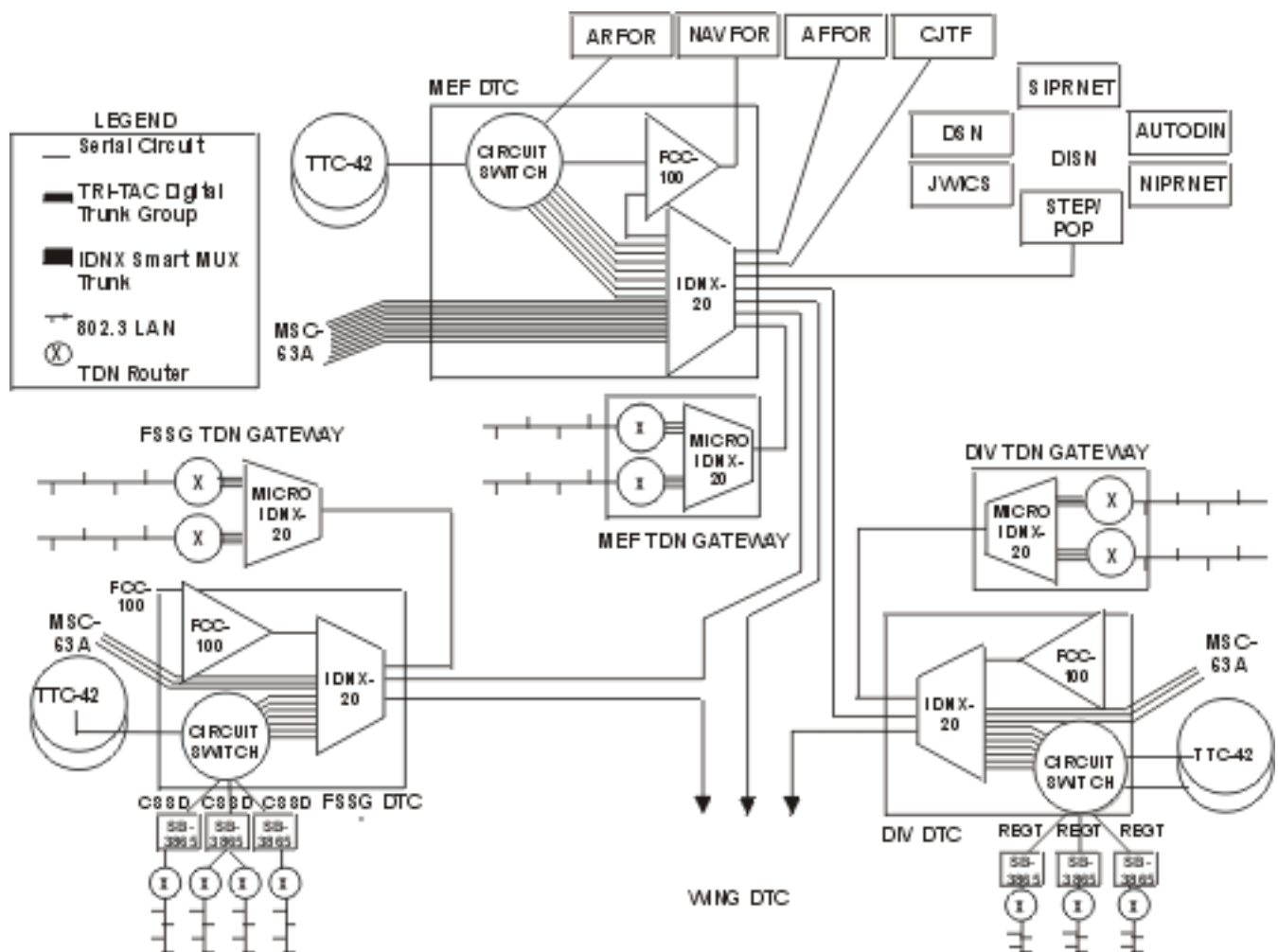


Figure 5-10. Smart Multiplexer Connectivity.

cannot operate on the move. Consequently, maneuvering elements will rely on SCR in most situ-

ations. Table 5-9 lists the MCRs employed by the MAGTF.

Table 5-9. MCRs

Category	MAGTF Radio	Type or Use
SHF terrestrial	AN/TRC-170(V)5	Troposcatter radio terminal
SHF SATCOM	AN/TSC-85B AN/TSC-93B	GMF satellite terminals
UHF terrestrial	AN/MRC-142	Line of sight radio
UHF SATCOM	AN/TSC-96A(V)	Satellite communications central
HF multichannel	AN/TSC-120	Communications central

a. SHF Terrestrial

The AN/TRC-170 is a microwave radio terminal developed under the TRI-TAC program. The AN/TRC-170 provides secure digital trunking between major nodes of the MAGTF communications network and limited dedicated circuits between individual subscribers. The AN/TRC-170 includes antennas, radio transmitting and receiving equipment, digital transmission group multiplexing equipment, digital and analog voice and data orderwires, and built-in test equipment for fault isolation. Although longer links have been successfully installed, the AN/TRC-170 nominally supports a 100-mile communications link. Link distance depends on the transmission technique used (mode of operation), data rate, terrain and horizon angles, and atmospheric conditions. Communication battalions and Marine wing communication squadrons operate the AN/TRC-170.

(1) Low Data Rate Multiplexer (FCC-100). The most important feature of the FCC-100 is its capability to conserve the conditioned diphase bandwidth and digital trunk group interfaces to the TRI-TAC system while providing a compatible interface to a commercial T1 multiplexer digital trunk group. Commercial and TRI-TAC interface capabilities are available on both the loop and trunk group sides of the FCC-100. It interfaces with a single group of the digital group modem and provides up to 16 loop ports. These loop ports can be a mix of synchronous, asynchronous, isochronous, conditioned diphase data, and CVSD and pulse-code modulation voice frequency (analog-to-digital and digital-to-analog) signals. With the appropriate interface card, two-wire foreign exchange systems and four-wire voice compression coder-decoder (CODEC) modules, STU-III, facsimile, and modem interfaces are supported. Characteristics of the AN/TRC-170 are listed in table 5-10.

Table 5-10. AN/TRC-170 Characteristics.

Characteristic	AN/TRC-170 (V) 5
Frequency range	4.4 - 5.0 GHz (tunable in 100-kHz increments)
Bandwidth	3.5 or 7.0 MHz
Transmitter power	1 kW
Diversity	Dual
Data rates	Up to 4,608 kbps
Channel capacity (at 32 kbps)	Up to 144 (includes overhead)

(2) Modes of Operation. The AN/TRC-170 can be operated in one of three modes with various ranges achievable in each mode. The modes are line of sight, troposcatter, and obstacle gain diffraction. Each mode is useful under certain circumstances and in various environmental conditions. The extensive capabilities and flexibility of this system make it an invaluable transmission system and workhorse that provides the connectivity between the MSCs and the CE of the MEF.

Line-of-sight mode requires minimal power output (down to 0.25 W) and requires straight-line clearance between sites. Normally, line of sight is used for links up to 10 miles. Figure 5-11 depicts this mode of operation.

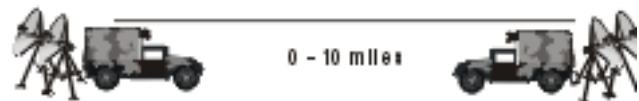


Figure 5-11. Line-of-Sight Mode.

Troposcatter mode is used for link distances of 40 to 100 miles. Ranges of up to 150 miles are possible with troposcatter, and ranges of under 75 miles, while possible, are difficult to achieve. A small portion of the transmitted radio waves is refracted off the troposphere toward the distant-end AN/TRC-170. (See fig. 5-12.)

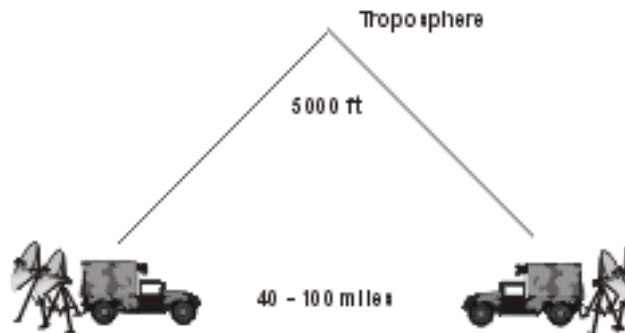


Figure 5-12. Troposcatter Mode.

Obstacle gain diffraction mode is used for link distances of 10 - 40 miles with an obstacle (e.g., a mountain) located between the sites. Radio waves are diffracted off the obstacle toward the distant-end AN/TRC-170. (See fig. 5-13.)

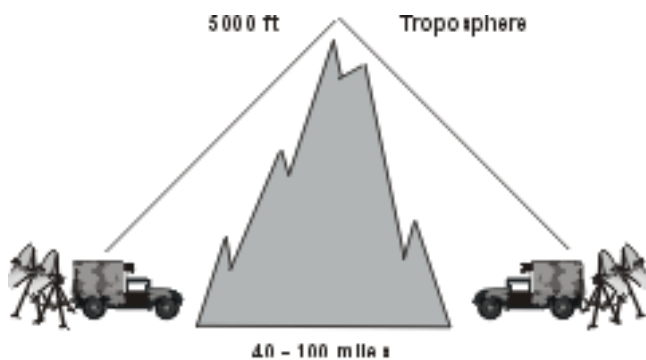


Figure 5-13. Obstacle Gain Diffraction Mode.

(3) Subscriber Channels. By using two loop group multiplexers (LGMs), up to 32 individual channels (any combination of digital and analog, depending on availability of circuit card assemblies) can be accommodated. These interface with the AN/TRC-170 through four-wire WF-16 or CX-4566 cable.

(4) Group Trunks. Up to four groups interface with the AN/TRC-170 through CX-11230 or fiber-optic cable.

(5) Potential TRC-170 Configurations. The TRC-170 has a variety of potential configurations, including:

Multitrunking Terminal. The multitrunking terminal is used to provide connectivity between multiple sites.

Through Relay. The through relay is used to extend the distance of a link or provide connectivity when terrain prevents a single line of sight, obstacle gain diffraction, or troposcatter link.

Terminal Site. The terminal site is the terminated end of a link.

Dedicated Subscriber. The dedicated subscriber is used for point-to-point telephone and/or data circuits.

LGM Used as an RMC. As an RMC, the LGM is used to provide tactical telephone service to distant sites. The LGM is programmed the same as two stacked RMCs off the switchboard (TTC-42 or SB-3865).

Figure 5-14 on page 5-28 shows how these configurations could be used to form part of a MAGTF network.

b. SHF SATCOM

SHF SATCOM is employed in the MAGTF by using GMF TACSAT terminals and preplanned DISN satellite and STEP access. These systems are deployed by the communication battalion in support of the MEF. The MEF uses two types of GMF TACSAT systems: the AN/TSC-85B and the AN/TSC-93B.

(1) AN/TSC-85B. The AN/TSC-85B is a full duplex nodal satellite communications terminal that is capable of interfacing with a single satellite. It transmits a single carrier and receives between one and four carriers.

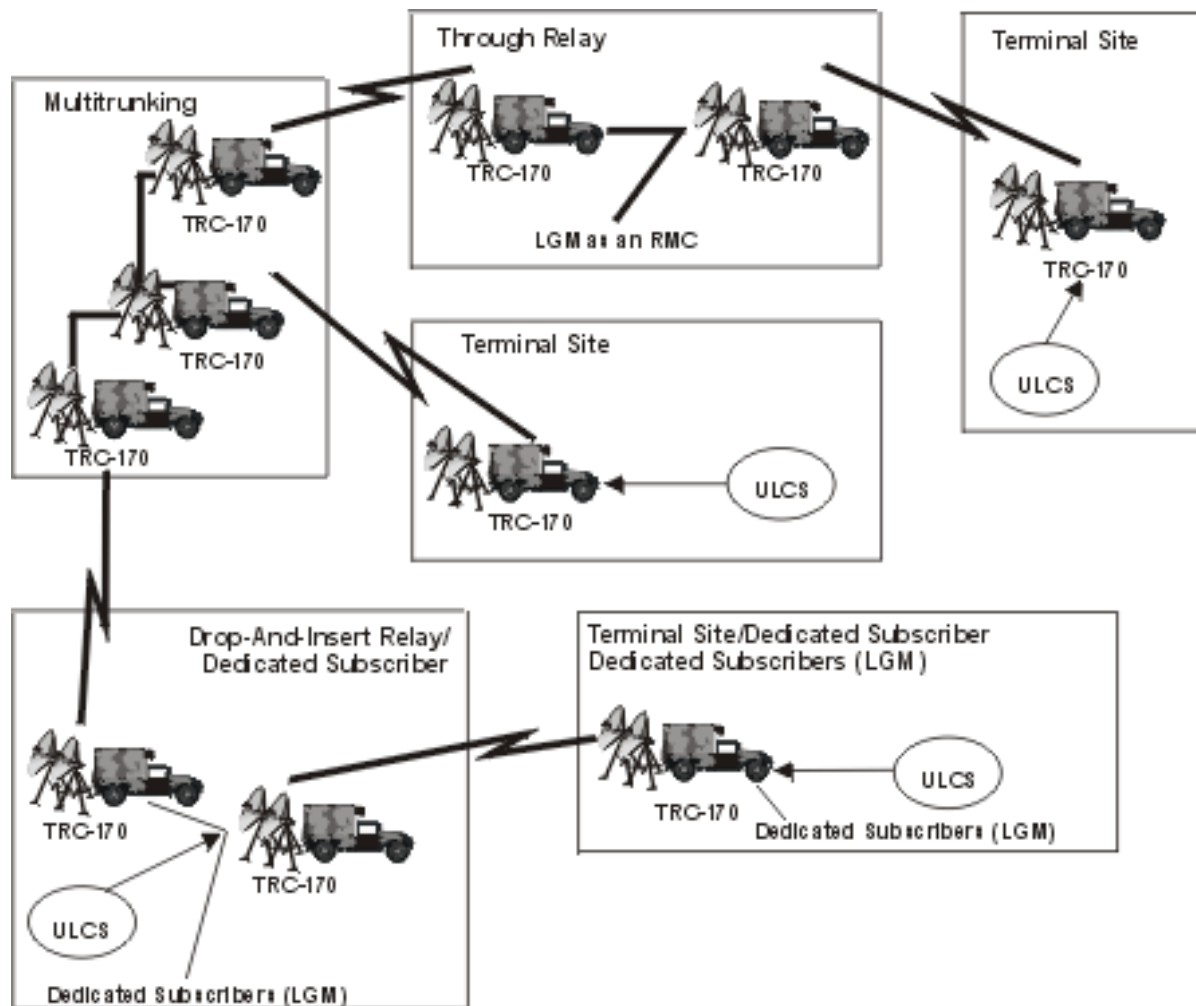


Figure 5-14. Notional TRC-170 Network.

(2) AN/TSC-93B. The AN/TSC-93B is a full duplex satellite nonnodal communications terminal. The TSC-93B simultaneously transmits and receives a single carrier.

(3) GMF TACSAT Capabilities. Table 5-11 lists the capabilities and characteristics of the SHF SATCOM terminal systems. Characteristics of the AN/TSC-85B terminal are the same as those of the AN/TSC-93B unless otherwise noted.

(4) Potential Configurations. A GMF network is composed of nonnodal and nodal terminals connected through a satellite to provide the user data communications links. System configurations

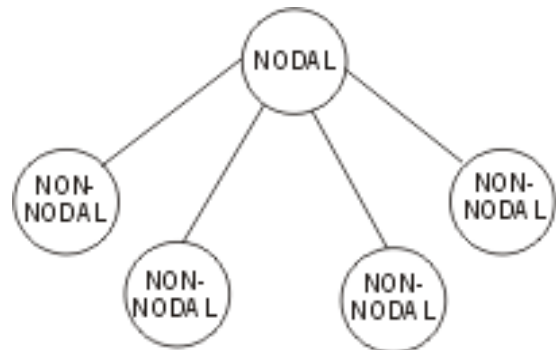
available with MAGTF GMF assets are point-to-point, nodal, mesh, or hybrid mesh/nodal.

In the point-to-point configuration, each terminal communicates with the other terminal only. All GMF terminals are capable of operating in this configuration. Associated cut sheets and terminal assignment sheets must be coordinated with detailed planning to ensure systems interoperability and minimize troubleshooting efforts. (See fig. 5-15.)

In the nodal configuration, the central or nodal terminal is able to communicate directly with all of the peripheral or nonnodal terminals. The AN/TSC-93B is a nonnodal terminal, and the AN/

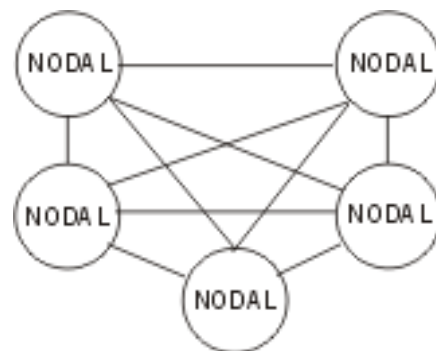
Table 5-11. SHF SATCOM Terminal Systems Capabilities.

Transmit frequency range	7900 - 8400 MHz	
Transmit bandwidth	40 MHz	
Power output	500 W (nominal)	
Receive frequency range	7,225 - 7,725 MHz	
Receive bandwidth	500 MHz	
	AN/TSC-85B	AN/TSC-93B
Group data rate		
Balanced nonreturn to zero (NRZ)	8 - 1,152 kbps	8 - 1,152 kbps
Conditioned diphase	72 - 1,152 kbps	8 - 1,152 kbps
Unbalanced NRZ	288; 576; 1,152 kbps	288; 576; 1,152 kbps
Low-rate multiplexer: (12 channels/ low-rate multiplexer)	8 low-rate multiplexers	3 low-rate multiplexers
Maximum data rate	256 kbps	
Minimum/maximum per channel	1,256 kbps	
TRI-TAC: (digital trunk group)	4 ports via group modem	1 port

**Figure 5-15. Point-to-Point Configuration.****Figure 5-16. Nodal Configuration.**

TSC-85B is a nodal terminal. The nodal terminals can communicate with up to four nonnodal terminals. (See fig. 5-16.)

(5) Mesh Operations. In this configuration, the nodal units communicate with each other. The AN/TSC-85B can simultaneously communicate with four other AN/TSC-100As or AN/TSC-85Bs with all terminals operated in a nodal mode. For communications to be possible, the baseband equipment must be compatible. (See fig. 5-17.)

**Figure 5-17. Mesh Configuration.**

(6) Hybrid Mesh/Nodal. In configuration, nodal units communicate with both nodal terminals and nonnodal terminals simultaneously. The AN/TSC-85B can communicate with any combination of up to four AN/TSC-100As, AN/TSC-85Bs, AN/TSC-94As, and/or AN/TSC-93Bs. The TSC-100A and TSC-94A are GMF terminals that the Air Force operates and provides for MEF and/or Marine component support under a formal MOU. (See fig. 5-18.)

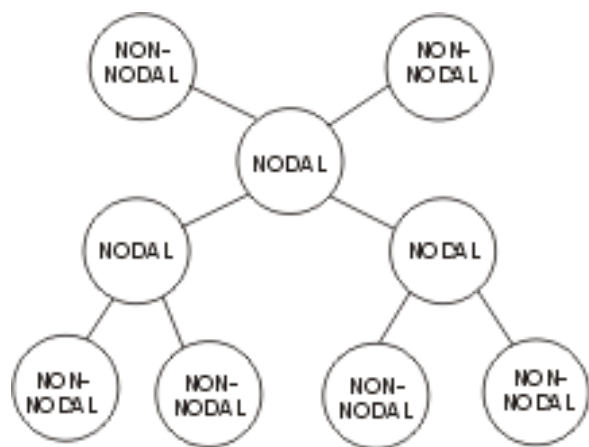


Figure 5-18. Hybrid Mesh/Nodal Configuration.

c. UHF Terrestrial

The AN/MRC-142 is the UHF terrestrial MCR terminal used by the MEF and its MSCs. A TRI-TAC-developed transmission system, the AN/MRC-142 is configured with two line-of-sight radio subsystem terminals. The line-of-sight radio subsystems can be set up to function as independent line-of-sight radio subsystem terminals or can be configured together to function as a through repeater or drop-and-insert repeater. Each line-of-sight radio subsystem terminal interfaces with another AN/MRC-142 line-of-sight radio subsystem terminal over a UHF radio link using parabolic grid antennas mounted on telescoping 50-foot masts. The characteristics of the AN/MRC-142 are provided in table 5-12.

Table 5-12. AN/MRC-142 Characteristics.

Frequency range	1,350 - 1,850 MHz
Bandwidth	100 (125 optional) kHz
Channel rate	144, 288, and 576 kbps
Output power	Low: 300 mW (25 dBm) High: 3 W (35 dBm)
Frequency stability	10 ppm
Orderwire channel	Analog: 300 - 3,400 Hz Digital: 16 kbps

The AN/MRC-142 has four operational configurations that provide the flexibility required of this system in MEF operations. It is capable of being configured as a single- or dual-link terminal, a through repeater, or a drop-and-insert repeater.

One of the two line-of-sight radio subsystem terminals in each AN/MRC-142 is used to configure a single UHF radio link. In this operational configuration, the radio terminal equipment designated "number 1" is used because it provides the best equipment access and communicates with just one other AN/MRC-142.

Two line-of-sight radio subsystem terminals in each AN/MRC-142 are used when two separate UHF radio links are required. In this configuration, the two independent radio terminals communicate with single line-of-sight radio subsystem terminals in two other separate AN/MRC-142s.

The through repeater configuration is used when a particular radio path between two AN/MRC-142s is longer than 20 - 30 miles or does not have a line-of-sight path. The through repeater configuration uses a third AN/MRC-142 to extend or complete the radio link between two communicating AN/MRC-142s.

The drop-and-insert repeater configuration is used when a particular mission requires access to traffic at a repeater site. The drop-and-insert function is accomplished by connecting a TD-1234 RMC between the cable side interface of the two line-

of-sight radio subsystem terminals. In this mode, a digital transmission group from one end is put into the high group side of the RMC. The RMC demultiplexes eight individual traffic channels from the group and passes on a low group, which is still combined. This combined low group is connected from the RMC to the second line-of-sight radio subsystem terminal and passed on to the distant end. The result is that eight channels from the source are “dropped off” at the repeater site and an additional eight channels (combined low group) are passed on to the distant-end terminal.

d. UHF SATCOM

The AN/TSC-96A(V) is a UHF SATCOM central terminal that provides the capability to receive and transmit GENSER message traffic. This system accesses AUTODIN through the Naval Common User Digital Information Exchange Subsystem (CUDIXS) and provides access to secure voice communications and fleet broadcast via UHF satellites. It can be employed anywhere in the world within the coverage of any fleet satellite (FLTSAT), UHF follow-on satellites, leased satellite, or GAP FILLER satellites.

The AN/TSC-96A(V) is a UNIX-based system hosted on two processors and workstations with Naval Modular Automated Communications Subsystem II (NAVMACS II) software. It interfaces with the AN/MSC-63A, Banyan VINES servers, and PC-client software loaded on computer terminals for message distribution. The system has the capability to receive four high-speed fleet broadcast channels. It was designed with internal backup and the capability to remote DAMA secure voice up to 100 feet. The AN/TSC-96A(V) can use four DAMA ports and monitor four fleet broadcast channels. A daily communication status report lists the available channels on the satellite for fleet DAMA and fleet broadcast.

There are 16 total channels on the fleet broadcast network. One channel is used for timing and overhead, leaving 15 operational channels. Eleven of the fleet broadcast channels are secure and can be processed by the AN/TSC-96A(V). These are called common and overload channels. The com-

mon channel is the primary channel for fleet broadcast traffic. The overload channel will broadcast messages that could not be broadcast on the common channel because of overload. It will also rerun messages transmitted on the common channel.

SCI channels are automatically routed/forwarded to the SCI facility, to the AN/MSC-63A, or directly to the user. Two weather channels can be transmitted over fleet broadcast and processed in the AN/TSC-96A(V). A tactical intelligence (TA-CINTEL) channel can be received in the AN/TSC-96A(V) but not processed. United Press International and Associated Press International news are sometimes transmitted and can be processed.

The AN/TSC-96A(V) has several configurations available to the supported unit. The subsystems and capabilities/limitations listed above are available in any configuration. The AN/TSC-96A(V) can be configured as—

- A stand-alone communications message center
- Networked into an AN/MSC-63A message switch
- Networked into the LAN.

The AN/TSC-96A(V) can be configured to support a unit with all of the capabilities of a communications center except the reproduction capabilities. In this configuration, the AN/TSC-96A(V) provides primary AUTODIN entry via the associated NCTAMS. In addition to the GENSER message traffic capability, the AN/TSC-96A(V) can provide the using unit with a secure voice capability.

The AN/TSC-96A(V) can be connected to the AN/MSC-63A message switch for increased capabilities. In this configuration, the AN/TSC-96A(V) can provide the primary or secondary AUTODIN access for units connected to the AN/MSC-63A.

The AN/TSC-96A(V) can be linked into the LAN through several options. If the network users are

using PC-client software, the LAN can be administered through the AN/TSC-96A(V). If the network is using Banyan VINES software, a third computer terminal is needed between the servers. This terminal is the gateway between the Banyan VINES server and the TAC-3 server. This terminal requires Super TCP/IP and NAVMACS II software for the system to be compatible with Banyan VINES networks.

The AN/TSC-96A(V) uses the Navy UHF SATCOM system, which consists of information exchange and quality monitoring subsystems. Satellites relay communications and control information as well as data to manage satellite resources.

The subsystems are designed to address specific naval communications requirements. These subsystems provide various communications networks with specific services and capabilities.

(1) Fleet Satellite Broadcast Subsystem. This is an expansion of the fleet broadcast, which historically has been the central communications medium for operating naval units. Fleet broadcast is a receive-only function that allows the subscriber the ability to monitor 4 channels at 75 bps per channel. In addition, fleet broadcast can be used as an alternate route for receiving message traffic if the CUDIXS link is not available. High-speed fleet broadcast is available from NCTAMS. High-speed fleet broadcast gives the subscriber the ability to receive the four channels of fleet broadcast at 2,400 bps per channel.

(2) CUDIXS/NAVMACS II. These two systems combine to form a communications network for transmitting GENSER message traffic between ships and shore installations. CUDIXS is ashore, and NAVMACS II is aboard ship and in the AN/TSC-96A(V).

Secure Voice. This is a narrowband UHF subsystem that provides voice communications be-

tween ships and with wide-area voice networks ashore.

TACINTEL. This subsystem is specifically designed for special intelligence communications.

DAMA. This subsystem is designed to multiplex several subsystems, or users, on one satellite channel. This multiplexing has the effect of allowing more satellite circuits to use a single UHF satellite channel.

Satellite Monitoring. This subsystem provides users of the UHF satellite communications system with means to analyze and resolve system and equipment-related problems. The SATCOM signal analyzer is operational at NCTAMS.

e. Super High Frequency (SHF) Tri-Band Advanced Range Extension Terminal (STAR-T)

The STAR-T (AN/TSC-156) is a HMMWV-mounted, multichannel, tri-band SATCOM terminal that will be fielded in FY 99. The STAR-T supports the equivalent of four 1.544 Mbps circuits. It can communicate with the DSCS and commercial satellite systems. It is capable of wideband satellite transmission and reception over the DSCS. It is also capable of commercial satellite communications in the Ku and C bands of the electromagnetic spectrum. The AN/TSC-156 will replace the current inventory of AN/TSC-93(B)'s and AN/TSC-85(B)'s in the FMF. The STAR-T brings increased mobility, reduced set-up/tear-down times, and commercial access capability to the Marine Corps. The STAR-T will be organic to the Communication Battalion of the Marine Expeditionary Force. In addition to supporting the doctrinal MEF to Major Subordinate Command wideband links, STAR-T will provide smaller MAGTF's like MEU's the bandwidth they need to conduct a range of missions in the littorals. Maximum aggregate bandwidth on the downlink is equivalent to four 1.544 Mbps (T-1). It will have an increased channel bandwidth and greater operational capability.

f. Secure Mobile Anti-Jam Reliable Tactical-Terminal (SMART-T)

The SMART-T, a HMMWV-mounted, tactical SATCOM terminal, Nomenclature: AN/TSC-154. Scheduled for fielding in FY 99, this Extremely High Frequency (EHF) terminal is mounted on a HMMWV. It is capable of Low Data Rate (LDR) and Medium Data Rate (MDR) transmission and reception over the Milstar satellite constellation. The SMART-T brings a new capability to the Fleet- protected, survivable communications. It will be organic to the Communication Battalion of the Marine Expeditionary Force, and will also reside at the Communications Company of the Marine Division and the Communications Platoon of the Marine Infantry Regiment. SMART-T will also provide the means by which Marines participate in CINC and JTF mandated EHF communications circuits. Maximum aggregate bandwidth on the downlink is 1.544 Mbps.

g. HF Communications Central

The MAGTF uses the AN/TSC-120 for its HF interface to AUTODIN. It is a self-contained, stand-alone communications central used primarily for long-haul Defense Communications System entry and point-to-point, beyond line of sight communications. It provides connectivity for the major CEs of a MAGTF.

The AN/TSC-120 is shelter mounted on a heavy HMMWV. It may also include one AN/PSC-5 DAMA-capable UHF TACSAT radio per system. Each communication battalion maintains five AN/TSC-120s, which are operated in the 2–29.9999 MHz frequency range, with automatic tuning for 280,000 possible frequencies in 0.1-kHz increments. The AN/TSC-120 is capable of either single or double sideband operation. Its internal modems are capable of emulating several modems currently used in the DOD inventory,

making the AN/TSC-120 a highly interoperable and flexible system. Each modem is limited to emulating one modem-mode at a time, and only one modem can be patched per sideband.

AUTODIN interface is provided by using a laptop computer that provides Modes I, II, and V AUTODIN access. It can transmit and receive Joint Army, Navy, and Air Force Publication (JAN-AP)-128 messages at data rates of up to 2,400 bps (Modes I and II) and 1,200 bps (Mode V). Allied Communications Publication (ACP)-126 and message text format editor messages stored on 3.5-inch floppy disks can be modified, stored, and then transmitted.

Automatic link establishment automatically selects an optimum HF communications channel from an available list of approved, preprogrammed channels. It then executes a handshaking protocol to connect two or more HF radio systems in a half-duplex link with minimal operator involvement. Automatic link quality analysis calculates the quality of available channels and displays the results in a numeric format. On the basis of the automatic link quality analysis results, the operator can establish the link on the best overall channel or allow automatic link establishment to establish the link on the first channel that allows for communications. Once the link is established, the operator must choose the best channels for transmitting and receiving in order to establish the full-duplex link.

h. MEF Use

Through task-organization, the MCR equipment can be used at any location and with any unit in the MAGTF. However, the most common use of this equipment within a MEF is as shown in figure 5-19 on page 5-34. CJCSM 6231.04, *Joint Transmission Systems*, provides detailed information about the operation of MCR equipment.

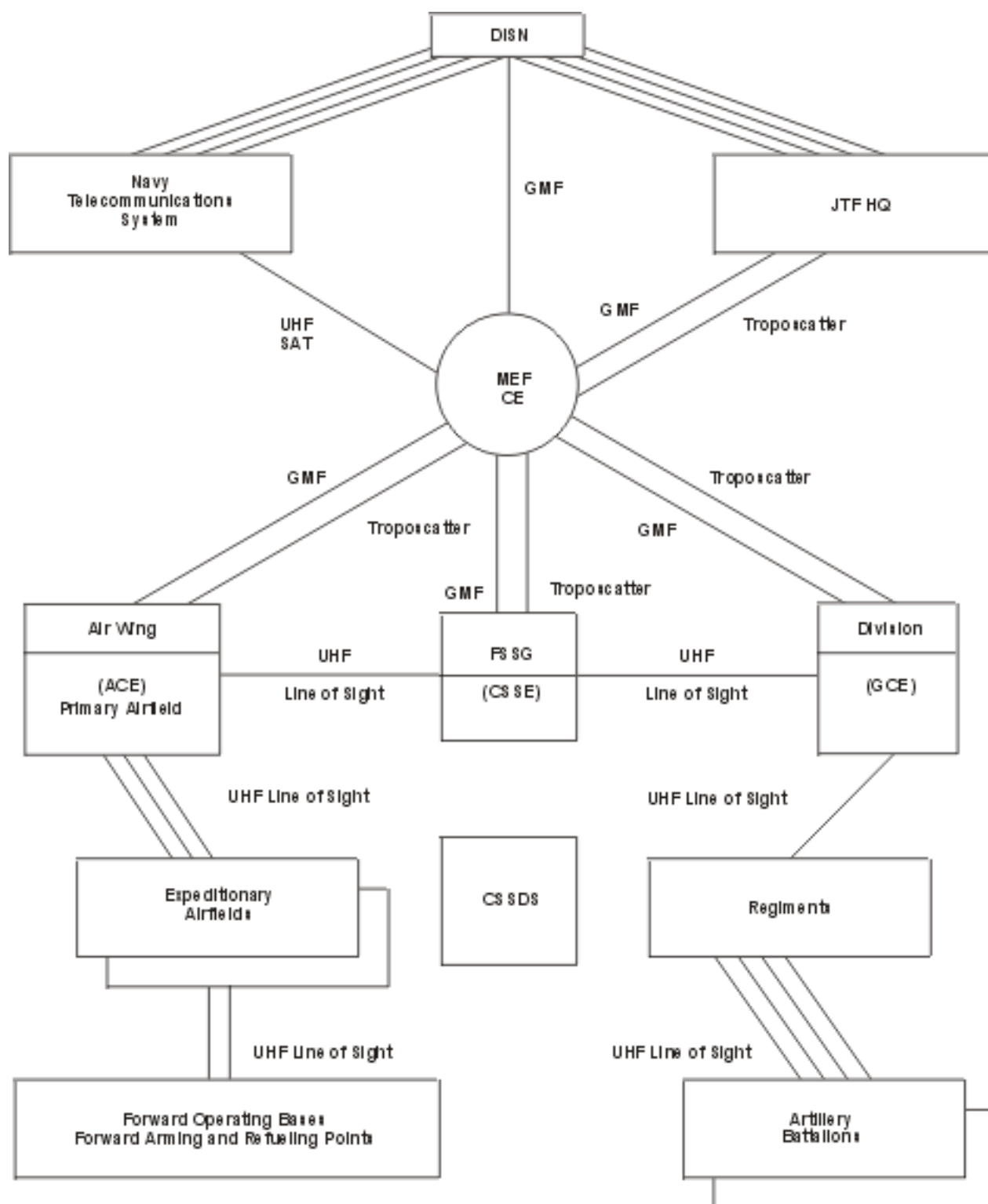


Figure 5-19. MEF Notional MCR Connectivity.

Section V

Special Purpose Systems

The MAGTF special-purpose system assets are systems designed to provide specific position location, navigation, information distribution, and cooperative identification services. These systems serve all MAGTF elements, often through externally managed satellite and aircraft relay systems. These systems provide real-time information to tactical users at the point of need.

5501. PLRS

PLRS provides MAGTF commanders with near real-time, accurate, three-dimensional position location and navigation information. It is a time-ordered, spread-spectrum radio system operating in the Ultra-High Frequency (UHF) band between 420 and 450 megahertz. Integral error detection and correction, cryptographic security, and frequency hopping features provide resistance to electronic countermeasures.

The PLRS radio set can be employed in the following configurations: manpack, surface vehicle, or aircraft. The five-ton truck configuration of the current PLRS Master Station is being replaced by the Net Control Station-EPLRS (Downsized) (NCS-E[D]). The NCS-E(D) improves mobility, flexibility, and reliability. It can accommodate up to 460 radio sets in a single PLRS “community.” Key planning considerations are the number and location of “reference” radio sets and the location of relays, as necessary. (Each radio set in the network is capable of automatically relaying data to the NCS-E(D) without operator action.) Reference sites can be surveyed, in which case they are fixed, or established by using a Global Positioning System interface, which provides additional mobility and versatility.

PLRS is employed by PLRS Platoon, Communications Company, Marine Division. The U.S. Army (Enhanced PLRS [EPLRS]), U.S. Navy (AN/KSQ-1), and U.S. Air Force (Situational Aware-

ness Data Link [SADL]) also have PLRS-related requirements.

5502. Precision Lightweight GPS Receiver (PLGR)

The AN/PSN-11 PLGR is a small, handheld, GPS receiver that weighs approximately 3 lb. It provides precise positioning and timing solutions based on signals received from the GPS satellite constellation. Position can be displayed in virtually any format, including latitude/longitude, military grid reference system, and Universal Transverse Mercator. It contains 49 map datums, and users can program way-points for navigation with back azimuths and distances to the next way-point available with the push of a button. The PLGR is compatible with night vision goggles. It is important, however, to understand the difference in capabilities between the PLGR and PLRS. While the PLGR provides a dramatic improvement in land navigation capability, it cannot provide the location of another unit and has no communications capability beyond the passive receipt of location and time. It should be viewed as a complement for, not a replacement of, PLRS.

5503. JTIDS

JTIDS is an advanced radio system that provides information distribution, position location, and cooperative identification capabilities in an integrated form. The primary JTIDS mission is to coordinate tactical resources for air defense of the MAGTF. JTIDS is a spread spectrum, fast frequency hopping, cryptographically secure, digital (data and voice) communications system. The system operates in the 960–1,215 MHz frequency band and provides jam-resistant, line-of-sight communications using a time division multiple access (TDMA) architecture. The system has a maximum range of 500 miles. The Marine Corps

will implement the JTIDS terminal in the TAOM to enhance coordination of antiair warfare. The other services are fielding JTIDS in aircraft as well as in air defense command and control systems. JTIDS is also an integral component of NATO air defense systems.

5504. Integrated Broadcast Services

IBS is a worldwide, DOD standard network for transmitting tactical and strategic intelligence information and targeting data. IBS will integrate intelligence broadcast using the DII for both broadcast and interactive dissemination. IBS will migrate tactical terminals/receivers to a single, related Joint Tactical Terminal (JTT) family. The JTT Common IBS modules will enable seamless information displays on GCCS. The goal of IBS is to resolve the proliferation of stovepipe intelligence broadcast formats by providing the tactical commander with an integrated means of delivering intelligence information to the warfighter.

5505. Commander's Tactical Terminal

CTT (AN/USC-55) is a multi-service developed special application UHF satellite communications receiver that can be dedicated to receiving critical, time-sensitive intelligence to commanders and intelligence centers at all echelons, in near-real-time, at GENSER or SCI levels. Its receiver provides one full duplex and two receive-only channels. Planned concept of employment for CTT is similar to that of the tactical receive equipment (TRE); i.e., fielded widely within the MAGTF to allow access to intelligence broadcasts and intelligence collectors. Full operational capability for CTT is expected by the fourth quarter of fiscal year 1998.

5506. The Joint Tactical Terminal

JTT, with its common IBS modules, is capable of receiving diverse broadcasts into terminals with

common capabilities. These terminals use multiple communications transmission paths and sound information management to provide the ability for each user in the battlespace to view a common operational picture/common tactical picture. The modular feature of these terminals allows producers and users in the MAGTF to incorporate IBS into their existing CIS. Hardware and software existing in the MAGTF (IAS, TCO, ACE systems, etc.) can integrate the common IBS modules that add the required capability. Alternatively, users may also obtain completely configured tactical terminals. Employment of JTT/common IBS modules facilitates a seamless transition from current dissemination systems to the IBS without degrading the capabilities provided by the current systems.

5507. TROJAN SPIRIT II

TROJAN SPIRIT II consists of two heavy HMMWVs with lightweight multipurpose shelters, trailer-mounted power generation units, and a towed 2.4-meter (C, Ku band) or 6.1-meter tri-band (C, Ku, and X band) antenna. The 6.1-meter antenna is not used by the Marine Corps. The second heavy HMMWV is used as a maintenance shelter. TROJAN SPIRIT II is a mobile, SHF SATCOM system that is capable of receiving, transmitting, and processing multimedia products, including imagery and secure dial-up voice, data, facsimile, and video.

TROJAN SPIRIT II will be deployed to provide GENSER and SCI communications for intelligence operations. TROJAN SPIRIT II provides 16 channels of digital voice or data when used exclusively for SCI or collateral secret traffic. This mode of operation allows a maximum T1 aggregate data rate. If both SCI and collateral secret traffic are handled, a 2-channel separation between SCI and collateral secret traffic results in a lower aggregate data rate. TROJAN SPIRIT II provides LAN communications supported by two separate Ethernet LANs (SCI and collateral secret) and entry to the SIPRNET and the JWICS.

5508. Global Broadcast System

The GBS will augment and interface with other CIS and provide a continuous, high-speed, one-way flow of high volume information to deployed or garrisoned Marine units. GBS will support routine operations, training and military exercises, crisis, situational awareness, weapons targeting, intelligence, and the transition to and conduct of opposed operations short of nuclear war. GBS will provide the capability to quickly disseminate large information products to various joint and small user platforms. GBS coverage will be worldwide.

5509. JTF Enabler Module

The JTF enabler provides the JTF, Marine component, or MEF commander an initial, in-theater, immediate, reliable command and control capability. Detailed guidance for the employment of CIS in support of joint operations is found in JCS Pub 6-0, *Doctrine for Command, Control, Communications, and Computer Support to Joint Operations*; JCS Pub 6-02, *Joint Doctrine for the Employment of Operational/Tactical Command, Control, Computer, and Communications Systems*; and the CJSM 6231 Series, *Manual for Employing Joint Tactical Communications*.

The module includes the personnel and equipment needed to establish high-capacity, long-haul communications links and provide information systems services. This capability would be used by the JTF, Marine component, or MEF com-

mander to support preparations for the introduction of follow-on forces. The Marine Corps currently augments MEU(SOC)s with this capability. In coordination with the commander of the amphibious squadron, the organic CIS of the amphibious ready group and the embarked MEU(SOC), augmented with an enabler module, can support initial command and control of follow-on forces from either afloat or ashore.

The JTF enabler includes the GCCS deployment and operations modules, such as the JMCIS/TCO module; the CTAPS; the JDISS; and secure electronic messaging. Currently, an AN/TSC 93B(V)1 is used to provide high-capacity, long-haul connectivity. The personnel and equipment for the enabler are currently provided from the organic assets of the supporting comm battalion.

The JTF or follow-on forces enabler allows a JTF, Marine component, or MEF commander to fall in on assets carried by a forward-deployed MEU(SOC) and commence operations without delay. The MEU(SOC) can provide limited command and control systems support ashore for a short period of time. The responsibility for CIS support for the JTF HQ shifts to the JCSE and the JTF HQ organic information systems support upon their arrival in theater. The JTF enabler module will usually backload with the MEU(SOC) upon arrival of sufficient JTF HQ assets and capabilities in order to be ready for employment as an enabler for additional follow-on forces. The enabler module, however, may also remain as part of the MEF CE or Marine component HQ.

Chapter 6

Planning and Execution

Effective C2 depends on the effective and efficient operation of CIS. These systems provide the means to develop a common operational picture (COP); to prepare and rapidly disseminate OPLANs and OPORDs; and to monitor, direct, and coordinate maneuver, fires, and logistics. In turn, the effective, efficient operation of these CIS depends on detailed planning that is thoroughly integrated with the operation planning process. Coordination and integration are key to ensuring development of OPLANs that are supportable from a CIS perspective and CIS plans that are responsive to the needs of the operation. Normally, the commander assigns the responsibility for detailed preparation of CIS plans and orders to the G-6/S-6, who is the CISO.

The CISO should be thoroughly familiar with the form, content, and techniques for preparing these documents. This chapter describes the planning process as it pertains to the CISO, establishes basic planning guidance, discusses planning considerations, and describes CIS planning documents. This information is provided to assist the CIS planner in participating in the overall operation planning process and in preparing CIS plans that are complete and effective and that support the mission of the MAGTF and the Marine component.

Section I

Overview

Preliminary planning is conducted before the receipt of a mission. It is based on the analysis of facts and trends to predict probable commitments and to anticipate what action will be required to accomplish future tasks. Preliminary planning makes use of available information and logical assumptions to prepare studies, estimates, and plans. The depth of these studies, estimates, and plans is based on the time available. They are refined as more information becomes available and are the basis for subsequent planning. Other measures that may be taken to reduce planning time include the use of existing SOPs, concept plans (CONPLANs) and OPLANs that can be tailored and refined. Once a mission is received, operation planning involves six steps:

- Mission analysis.
- COA development.
- COA analysis.
- COA comparison/decision.
- Orders development.
- Transition to execution.

MCWP 5-1 (draft) provides the details of the Marine Corps planning process.

All planning is time constrained. To maintain operational tempo, an organization must employ techniques that reduce the overall time required to plan. Effective employment of information systems and information management procedures

permits concurrent, collaborative planning among staff sections and between echelons. This speeds up the planning process and, at the same time, results in better coordinated plans.

6101. Planning Information

The CISO collects and analyzes all available information relative to the impending operation and the resources available to support the operation to provide the commander and other staff members with sound advice for the employment of CIS. The CISO uses this information as the basis for estimating the situation, making recommendations, and preparing CIS plans.

a. Commander

The commander briefs the staff and subordinate commanders on the mission as part of the mission analysis. This briefing includes the action to be accomplished as well as the commander's intent, which describes the desired end state. At the end of the mission analysis, the commander provides initial planning guidance: the results of the mission analysis, necessary assumptions and constraints, COAs to be considered, and any other considerations that may influence planning. After issuing this guidance, the commander keeps the staff and subordinate commanders informed on a continuing basis as mission-related information is received and decisions are made.

b. Staff

The CISO is the G-6/S-6 and, in this capacity, has staff cognizance for the overall CIS effort. The CISO must have continual interaction both with other staff officers and with supporting and subordinate CIS unit commanders. CISOs must obtain essential information from other staff members to understand and support the developing situation. Information that affects the employment of CIS must be aggressively pursued. Close coordination is critical to the establishment of effective C2.

c. Other HQs

The CISO must obtain information from other HQs during planning. Higher HQs may provide CIS support, impose special communications requirements, or issue special communications instructions for the operation. Subordinate HQs may require additional personnel, equipment, or other assistance to accomplish their mission.

6102. Coordination

Planning must be coordinated not only within the local command, but with the HQs of senior, subordinate, adjacent, supported, and supporting units. The proper coordination of planning efforts involves the prompt, continual exchange of information, decisions, plans, orders, and instructions among all interested parties. Coordination means include—

- Liaison with all personnel responsible for the exchange of planning information and coordination of planning activities.
- Interaction among G-6s/S-6s and communications units and detachments.
- Appropriate coordination and dissemination of information by staff sections.
- Coordination of planning documents.
- Staff conferences for the exchange of information between HQs and development of mutually-agreed-upon COAs.
- Timely briefings to keep the commander and staff informed of the current situation.

6103. Security

Operational security, COMSEC and COMPUSEC are important considerations during the planning of any operation. To maintain surprise, it is necessary to deny the enemy prior knowledge of details pertaining to an operation. Measures must also be instituted to control access to information and protect information systems and communications networks.

6104. Estimates

The CIS officer prepares estimates to assist the commander in the analysis of alternative COAs. On the basis of factors such as terrain, weather, distance, scheme of maneuver, and availability of personnel and equipment, the CISO predicts the supportability of COAs from a CIS perspective. The CISO also provides the commander with recommendations on how the available means can best support the selected COA. Formal, detailed, written estimates are usually prepared only during preemployment. Once execution begins, written estimates are seldom used. Whenever the situation warrants, a revised estimate is briefed to the commander and/or other staff officers for their consideration in the planning process. In either case, the CISO's estimate should derive from a logical sequence of thought that considers all critical elements of CIS planning. A suitable form for a formal CIS estimate is included in appendix I.

6105. Recommendations

The CISO makes recommendations to the commander, as required, to assist in establishing policies and making decisions. The CISO should also offer recommendations to other staff officers and subordinate commanders on CIS matters. Although the CISO may follow formal or informal procedures in arriving at and making recommendations, many of the recommendations are based on observations or mental estimates. Recommendations based on other written studies or formal estimates are usually submitted in writing. Whatever the procedure, recommendations are the product of careful analysis and comparison constrained by the time available. They are candid and objective, are based on the best information

available, and, when appropriate, are coordinated with other staff sections. Recommendations are concise and presented in a form that requires only the commander's approval or disapproval.

6106. Preparing Plans

CIS planning is simplified when it is considered in reverse order (e.g., when developing a C3 Systems Annex for an amphibious operation, first address the assault phase and move in reverse order back to the planning and embarkation phases). A wide range of planning considerations is covered in the next paragraph. The maintenance and use of a standing CIS Annex, Annex K, which can be tailored for specific operations, greatly facilitates the timely preparation of OPLANs. (See app. J.) The CIS procedures that remain constant, such as the MAGTF internal telephone numbering scheme, should not have to be re-planned regardless of the time, location, or type of operation. The CIS planner may then concentrate on specific requirements for a particular operation, with only a quick review of the other items that may have changed over time.

6107. Implementing Plans

Once a CIS plan or annex is completed and approved, it must be implemented effectively. Close supervision and frequent examination of the status of information systems and communications networks by the CISO and staff are essential. Plans will inevitably be modified as the operational situation develops. The CISO and staff must keep abreast of developments and be prepared to adapt the CIS plan to the changing situation to support and maintain MAGTF operational tempo.

Section II

CIS Requirements

The CISO must determine the resources required to support the operation and request augmentation if needed. To do this, the CISO must first determine the information processing and information transfer requirements to be supported. This involves extensive coordination with CISOs of higher, subordinate, adjacent, supporting, and supported units. All aspects of the operation must be considered to accurately determine the requirements for information processing and information exchange.

6201. Mission

The mission statement describes, in concise terms, the location of the operation, the time it will occur, and the tasks to be accomplished. The mission includes the commander's intent—the purpose of the action. Careful review of the mission gives the CISO a general idea of what overall CIS resources will be required to support the operation. At the component level, the possible designation of the Marine component commander as a functional component commander or the possible requirement to provide the nucleus of a JTF HQ would drive a significant increase in CIS requirements.

6202. Courses of Action

A COA is an approach to accomplish the mission. The CISO develops estimates of supportability for each COA considered while at the same time influencing COA development on the basis of CIS capabilities and limitations.

6203. Concept of Operations

The concept of operations generally depicts the scheme of maneuver, the employment of support-

ing fires, and in an amphibious operation, the landing plan. Analysis of the concept of operations gives the CISO an understanding of when events will occur, projected locations and movement of units and C2 facilities, and the distances the communications network must span.

6204. Task Organization

The task organization lists all tactical, administrative, and service groupings with the commanders of each. It depicts the organization for combat and indicates the command relationships of the assigned forces. Review of the task organization helps the CISO determine the requirements for internal and external information flow to be supported by the communications network. Review of the task organization also enables the CISO to identify the C2 facilities and their associated requirements for information systems support. A major consideration is whether the component and the MAGTF commanders are supported by separate staffs and, if by separate staffs, whether or not those staffs are collocated. The requirement to support separate, geographically separated, component and MAGTF CE HQs will severely stress the capabilities of a communication battalion.

After the CISO has determined the requirements to be supported, the factors that may affect the employment of information systems and communications networks are analyzed. These include:

- Available resources.
- Enemy situation.
- Environment.
- Information management plan.

6205. Available Resources

The CISO must consider all available resources to determine the extent of support that can be provided and to determine shortfalls in the capability to support the mission. This includes resources both organic and external to the MAGTF.

a. Personnel

The number, military occupational specialties, state of training, and availability of replacements are of primary concern. Individual mobilization augmentee billets must be filled, contractor support requirements must be identified and, when appropriate, agreements for other-Service augmentation must be exercised.

b. Equipment and Services

The availability, condition, and operational characteristics of equipment must be identified, as must the availability of external telecommunications services. This includes identifying equipment available through joint or other-Service augmentation and telecommunications services available through commercial sources, and, in some cases, host nation support. Points of contact for information concerning the employment and maintenance of equipment should be researched in advance of operations. The Marine Corps Systems Command, the Marine Corps Network Operations Center (NOC), the Command and Control Systems School, and the Marine Corps Communications-Electronics School are excellent sources of information, as are equipment manufacturers and suppliers. Information on interfaces to joint, other-Service, allied, commercial, and host nation equipment should be researched.

c. Software

The compatibility and interoperability of CIS are major concerns. Even in a single information or communications system, different versions or releases of software may be incompatible. For example, various versions of the GCCS (JMCIS Unified Build and MAGTF C4I Software Baseline) are not compatible and can preclude information sharing between the embarked MAGTF and shipboard systems. In Operation Desert

Storm, newly fielded TRI-TAC equipment required extensive software modifications to achieve interoperability between Services and with joint HQs. The CISO must ensure that users of CIS are aware of the potential for incompatibility and take appropriate action to ensure that systems are interoperable and compatible. MCTSSA is responsible for software support of fielded systems, and MEF CISOs should coordinate with MCTSSA to implement new releases of software and to identify and resolve software problems.

d. Supplies

The quantity and condition of available supplies such as wire, batteries, and repair parts, and the availability of resupply in the objective area need to be coordinated.

e. Maintenance

Maintenance requirements must be anticipated and support planned for each phase of the operation. Particular attention to the availability of test equipment is necessary to support maintenance efforts in the objective area. Planning must take into consideration the availability of maintenance support through inter-Service agreements and host nations.

6206. Enemy Situation

Enemy intelligence, reconnaissance, and EW capabilities can significantly degrade and in some cases exploit our CIS. The potential for disruption of MAGTF command and control must be understood and countered. The CISO should always assume that the enemy has the capabilities to intercept, locate, exploit, deceive, and/or otherwise degrade MAGTF CIS. The enemy threats can be countered through—

- Threat awareness.
- Sound COMSEC and COMPUSEC procedures.
- Restricted RF emissions.
- Employment of secure, jam-resistant, low-probability-of-intercept transmission equipment.

- Use of wire and messengers.

Chapter 7, sections I and II, address COMSEC and COMPUSEC.

The CISO must take into consideration the threat capability to employ NBC weapons. Given the continued proliferation of weapons of mass destruction to both outlaw nations and non state actors, even military operations on the lower end of the conflict spectrum may include their use. Consequently, the CISO must plan for CIS support in a contaminated environment and be prepared to provide rapid decontamination of CIS equipment and facilities. (See app. K.)

6207. Environment

The CISO must consider those physical characteristics such as terrain, weather, and the electromagnetic environment of the objective area that may affect the employment of CIS.

a. Terrain

The CISO should be aware of the topography, vegetation, road networks, soil conditions, and other terrain features in the objective area. The terrain has a major bearing on the location of facilities, sitting of antennas and relays, effective range of line-of-sight transmission systems, installation of wire lines, and effectiveness of messenger service.

b. Weather

The climatic conditions in the objective area determine the requirements for special equipment or supplies such as heaters, air conditioners, shelters, or cold weather batteries. Many CIS do not operate effectively under conditions of extreme heat or cold, and heavy precipitation can adversely affect radio transmissions. The CISO must plan to operate under all weather conditions that will be encountered during the operation.

c. Electromagnetic Interference

The CISO must take into account the electromagnetic environment in the AO. Electromagnetic in-

terference, both natural and manmade, can severely degrade the performance of communications systems. An effective training program for operator and maintenance personnel is the key to being able to communicate effectively in an adverse electromagnetic environment. Information on the electromagnetic environment may be obtained from the Joint Spectrum Center and in MCRP 6-22B, *MSP for Spectrum Management in a Joint Environment*.

d. Facilities

The CISO should take into account the infrastructure in the AO, especially telecommunications and electric power generation and distribution facilities, and its potential availability either through host nation support or capture.

6208. Information Management Plan

The information management plan describes the processes by which information will be created, processed, maintained, and disseminated within the organization. Normally, the information management plan will consist of a set of SOPs that are updated as necessary to fit the circumstances of a particular exercise or operation and promulgated as an annex to the OPLAN or OPORD. The unit information management officer, with the guidance of the C/S or XO, and in coordination with the information management officers of each staff section and subordinate units, develops the information management plan. The CISO must ensure that the employment of CIS support the information management plan. The information management plan will include the following:

- Procedures by which information requirements are identified, developed and prioritized, including how CCIRs are nominated, approved, collected, reported, maintained, and disseminated. The information management plan will identify and assign responsibility for standing CCIRs (key items of information that will be required in almost any situation). Standing CCIRs must be reviewed for relevancy and modified, expanded, or deleted as necessary.

The CCIR procedures will include guidance on filtering and fusing raw data before submission and dissemination.

- Procedures by which the COP is maintained and shared. This will include guidance on the level of detail (e.g., a division COP might display friendly units down to the battalion level, and a battalion COP might display friendly units down to the platoon level); assignment of responsibility for the quality and integrity of the COP database, including the management of air, ground, and sea tracks/unit locations; and assignment of responsibility for maintaining the status of friendly and enemy units. Each staff section will be assigned responsibility for providing status information for the functional areas over which they have cognizance.
- Designation of data standards, including standards for symbology, report/message formats and data element standards.
- Procedures supporting the effective flow of both routine and time-sensitive information:
 - Automated networking techniques such as news groups, home pages, and other Internet-like methodologies.
 - Policy governing the use of e-mail.
 - Supply-push and demand-pull approaches to information dissemination, as well as echelon skipping where appropriate (e.g., re-supply requests bypassing intermediate echelons).
 - Manual as well as automated procedures for handling information dissemination. Tactical echelons must avoid overloading communication circuits. Particular attention should be given to the best approach for transferring high-volume data formats such as imagery, video, maps, and overlays. Messengers and hard copy OPODs remain a reliable means of information dissemination.
 - Procedures for the design, maintenance, access, use, synchronization, and integration of databases supporting command and control.
 - Procedures and schedules for daily briefings, meetings, and reporting. This daily operations cycle is developed in coordination with all staff sections and subordinate units. Upon commencement of operations, the C/S or XO may modify the operations cycle as necessary to maintain tempo or to adjust to the unfolding situation.

Section III

Pre-Deployment Preparation

Mission accomplishment often depends on pre-deployment planning and preparation. Numerous actions must be accomplished by the G-6/S-6 before deployment. Appendices C, F, G, H, and K of this publication and CJCSM 6231.07A (app. G), contain pre-deployment checklists that should be considered for incorporation into unit SOPs.

6301. Review Existing Plans and Orders

OPLAN and OPORD communications-electronics/CIS annexes, time phased force deployment data (TPFDD) files, planning guidance, and any other appropriate documentation, including after-action reports and CIS annexes from previous operations of a similar nature and unit SOPs, should be reviewed. Items not covered adequately in existing OPLANs or OPORDs should be identified. The CISO should prepare and submit updated information for the TPFDD file.

6302. Prepare Troop and Equipment Lists

Personnel requirements must be determined and the troop list prepared. The troop list should include rank, military occupational specialty, line number, and billet description. The CISO should determine equipment requirements and prepare an equipment list summarizing all Class VII items to be deployed.

6303. Request Augmentation

Augmentation of personnel and/or equipment should be requested if shortfalls exist in either area. The CISO must be familiar with any existing

memorandums of agreement for support from other Services and the procedures for exercising those agreements, as well as procedures for obtaining support from the Reserve. At the present time, both the Army and the Air National Guard have memorandums of agreement in effect with the Marine Corps to provide a portion of the communications equipment and personnel required to support two Marine component HQs.

6304. Coordinate Frequencies

The type and number of frequencies required should be identified in sufficient time and forwarded to the frequency manager who is found at, but not limited to, the joint, CINC, Force, MEF, and Base levels. Liaison should be made with the frequency coordinator so that required frequencies can be obtained, assigned, and distributed in sufficient time. The frequency coordinator provides guidance on frequencies used in garrison, during embarkation, in transit, and in the AO.

6305. Request Satellite Access

The CISO should identify requirements and coordinate requests for UHF and SHF satellite access through the frequency manager.

6306. Compile a Publications Library

General and technical publications need to be embarked to ensure that deployed units have access to the information they need. It may be advantageous to maintain some publications on mass storage media. However, essential publications should be available in hard copy.

6307. Initiate Telecommunications Service Requests

To request U.S. or host nation commercial resources, a telecommunications service request must be submitted. The telecommunications service request format is found in various DISA Circulars and should also be included in the unit CIS SOP. Telecommunications service requests are normally submitted via the chain of command well in advance of the operation.

6308. Conduct Communications/Command Post Exercises

These exercises are designed to test personnel and equipment readiness. In a communications exercise, the viability of the communications network is tested. In a CP exercise, unit staff functioning and information systems support are exercised to prepare for an operation. The optimal way to test both the staff and the adequacy of CIS support is by combining these two exercises. The staff become familiar with the information systems they will employ in the operation, and the CISO is able to test the adequacy of the communications network as well as the information systems support before operational employment.

6309. Provide CIS Support for Embarkation

Support is required throughout the embarkation phase. Movement to sea and aerial ports of embarkation requires communications nets for convoy control and coordination, and the actual embarkation of troops, equipment, and supplies is most efficient when supported with information systems. The preferred means of providing this support is through the use of equipment and personnel who are not deploying with the MAGTF.

6310. Submit Communications Guard Shifts

Upon deployment, a unit must submit a communications guard shift message to ensure continued receipt of its record traffic. Guard shift messages are used to update the Common Source Route File. Guard shift procedures are contained in naval tactical publication (NTP) 4, *Fleet Communications*. Deployed organizational and individual e-mail systems must also be established and redesignated for the deployment period.

6311. Request COMSEC Material

Requests for appropriate cryptographic material (equipment keys, etc.) must be expeditiously submitted through the appropriate chain of command to the controlling authority for each key required. The controlling authority validates the request and forwards it to the director of the Communications Security Material System for processing. The requisitioning process can be lengthy.

6312. Coordinate Logistics

The G-6/S-6, in close coordination with the G-4/S-4, must plan for logistic matters. The following areas require special attention.

a. Equipment

To ensure equipment readiness, limited technical inspections should be conducted on all equipment scheduled for embarkation. These inspections must be conducted as early as possible to allow time for correction of deficiencies before embarkation. Waterproofing and weatherproofing of equipment before deployment are essential to protect the equipment while in transit.

b. Power Requirements

The G-6/S-6 officer must identify to the G-4/S-4 the electrical power requirements.

c. Embarkation Material

Units should maintain materials required for construction of embarkation boxes to meet mission requirements.

d. Technical Representative Support

Because of technical sophistication, contract technical representatives from the manufacturer are required to maintain some critical low-density equipment. Technical representative support is available for exercises and operations but requires considerable lead time. Requests for such support should be submitted in accordance with current directives.

e. Hazardous Cargo

Hazardous cargo is any material that is prone to fire, explosion, or toxic seepage, thereby presenting an inherent danger to personnel and equipment as well as to ships and aircraft. This type of material must be identified, packaged according to existing transportation regulations, and certified by a competent authority. Many restrictions apply. It is critical that these matters be addressed before embarkation so that vital equipment and supplies are not rejected by loadmasters or combat cargo officers during embarkation.

f. Repair and Maintenance

Sustained operations result in the need to maintain and repair equipment. Required repair parts,

based on the equipment density list, must either accompany the deploying unit or be staged in the AO. In addition to repair parts, appropriate test equipment and maintenance personnel must be available. Regardless of the operational readiness of equipment at embarkation, it will deteriorate if not properly maintained during sustained operations. Required items are often held in a contingency block that is identified by need and held ready for issue on demand. It is the responsibility of the CISO to request this block through the supply officer.

g. Supplies

In addition to repair parts, the G-6/S-6 must ensure that adequate provision is made for re-supply of other critical, high-volume consumables such as batteries and petroleum, oil, and lubricants.

6313. Effect Liaison/Coordination

For the CISO to accurately assess requirements and plan the necessary CIS support, close liaison and coordination with senior, adjacent, supporting, and subordinate CISOs as well as other staff officers are essential. Appendix P and CJCSM 6231.07A, appendix A, identify liaison/coordination points of contact.

Section IV

CIS Plans, Orders, and Directives

CIS plans and orders describe how CIS will be employed to support the commander in the exercise of C2. The G-6/S-6 is responsible to the commander for preparing the following plans, orders, and directives:

- CIS SOPs.
- Communications-electronics operating instructions (CEOI).
- CIS plan.
- CIS estimate
- CIS concept.
- Paragraph 5 of the OPORD or OPLAN
- CIS Annex (Annex K).

The G-6/S-6 is often required to provide CIS guidance for inclusion in other annexes of an OPLAN or OPORD. This may include the air annex and the naval gunfire annex. Planners must ensure that all necessary CIS guidance and instructions are covered in Annex K, other designated annexes where certain CIS instructions are appropriate, or both. The practice of cross-referencing annexes without adequate harmonization can result in gross omissions of required CIS guidance. Plans and orders follow standard formats. For a detailed discussion of standard formats for OPLANs and OPORDs, see MCWP 5-1 (draft).

6401. Standing Operating Procedure

The SOP is one of several types of orders that the commander develops and uses to accomplish the mission. It is a set of instructions covering those features of operations that lend themselves to a definite or standardized set of procedures without

loss of effectiveness. The procedures are applicable unless ordered otherwise. The SOP reflects approved doctrine as published in current doctrinal publications, directives, and regulations, modified to satisfy local operating conditions and the policies of the command. The SOP is normally followed, but may be modified, tailored, or even completely discarded depending on the situation. In no way should the SOP be allowed to reduce flexibility and adaptability or to limit creativity and initiative. The SOP is usually referred to in the OPORD with exceptions identified. The amount and type of information to be included in an SOP must be carefully determined. Procedures must be clear and concise. In the absence of specific orders to the contrary, the instructions contained in the SOP are guiding. The SOP—

- Reduces the need for other types of orders and simplifies the preparation and transmission of orders.
- Simplifies training by establishing uniform practices for the unit.
- Promotes understanding and teamwork throughout the command.
- Facilitates and expedites execution of routine procedures.
- Minimizes confusion and error.

The scope of the SOP varies with the echelon of the preparing command. An SOP prepared by a division is broad in scope and provides essential instructions for all major elements of the division. The SOP of a subordinate unit applies only to that individual unit and its subordinate elements. As the scope of the SOP narrows, the amount of detail increases. For example, an SOP for a section is detailed, describing what each individual does and in what sequence with respect to the actions of other individuals in the section.

a. Format

Although there is no established format for an SOP, one of the two following formats is generally used. An SOP may be formatted as an all-inclusive document containing in the main body sections and paragraphs detailing the duties and responsibilities of subordinate units and, where applicable, of personnel. This format does not have annexes or enclosures. The other approach is to publish the main body of the SOP as a basic document containing instructions of a general nature with annexes for technical details and specific instructions for individual units and/or personnel. For example, the basic document could contain information for the communications battalion as a whole with annexes for different functional areas such as TECHCON and systems planning and engineering. SOPs prepared by subordinate units must comply with and be coordinated with pertinent parts of the SOP of the higher command. SOPs should not repeat practices or procedures governed by other directives or documents that are readily available to all elements of the command unless such repetition is required to clarify local operating practices.

b. Suggested Content

- References such as MCWPs, field manuals, technical manuals, regulations, and the SOPs and CEOI of higher commands.
- Planning checklists.
- Training instructions outlining general training standards. Detailed instructions are normally contained in quarterly training schedules.
- Information systems security instructions that address both COMSEC and COMPUSEC. Instructions should be limited to those that are applicable to all elements of the command and are not contained in the command CEOI, as the purpose of this section should be to develop and maintain CIS security awareness throughout the unit.
- Physical security instructions designed to develop an awareness for physical security and to promulgate and standardize physical security procedures throughout the unit.
- Instructions for the operation of communications centers, including location and procedures

for transmittal, receipt, and processing of record traffic.

- Procedures covering the exchange of organizational and individual e-mail. The authorization for use and the records to be maintained should be prescribed.
- Procedures for wire communications, including wire and cable installation practices; priority of installation; tagging procedures; general guidance pertaining to locations of switching, routing, and patching facilities; LANs and terminal equipment; and instructions governing the placement of calls. Also, inclusion of directory service information, guidance for obtaining service, and instructions for maintenance of equipment and lines should be considered.
- Instructions pertaining to the planning, installation, operation, and maintenance of SCR equipment and guidance for the composition and operation of radio nets, including those required for data communications. Information about data interface modules used with the radios and the advance planning required for frequency hopping radios and TACSAT communications should be included. Actions to be taken in the event of imitative communications deception or jamming should be defined.
- Instructions pertaining to the planning, installation, operation, and maintenance of the switched backbone that apply to all elements of the command. Detailed instructions on operations should be published in the SOP of the unit that owns the equipment. Joint and other-Service interfaces, means of entry into the DISN, and planning for TACSAT communications should be addressed.
- Instructions pertaining to the planning, installation, operation, and maintenance of LANs, including switch, router, and/or server planning, installation, operation, and maintenance.
- General procedures to be employed by all users for the planning, installation, operation, and maintenance of radio-wire integration facilities.
- Instructions pertaining to the general use and distribution of visual and sound signal devices (flags, lights, pyrotechnics, panels, arm-and-hand signals, whistles, sirens, bells, voice amplifiers, explosive devices, etc.).

- Procedures to be followed to obtain frequencies, restrictions on the use of frequencies, procedures for reporting interference, and conditions under which radio silence is required.
- Instructions covering the identification of circuits and systems for installation and control purposes.
- Special communications support procedures (e.g., R and Y routers) that may be required for intelligence systems in the command.
- Identification of the various command, control, and coordination agencies, centers, and cells (this manual refers to these entities generically as command and control facilities, for example, COC, DASC, FSCC, TACC, and TAOC) within the command and their requirements for information systems support and communications connectivity.
- General procedures to be employed by all users for the planning, installation, operation, and maintenance of general-purpose computers and general guidance for interfacing all tactical information systems into the communications network. Detailed instructions on the operation of individual tactical information systems should be published separately.
- General instructions pertaining to communications control not covered elsewhere in the SOP. More detailed instructions on communications control will be promulgated in the CIS SOPs of communications units.
- Information pertaining to the location of the CISO and C2 facilities, selection of CPs, instructions governing the preparation of the CEOI, subordinate unit SOPs, and instructions pertaining to CIS planning for future operations.

c. Communications Units

The CIS SOP for a communications unit is unique in that it addresses the operation of the unit in the execution of its primary missions. Its scope is determined by the type of unit, the amount of detail the unit commander desires, and the echelon of command to which the unit is assigned. As a minimum, the SOP should include—

- Specific responsibilities of each major subordinate element.
- Instructions on routine operations of such importance that continuing instructions are desirable.
- Instructions governing the execution of all responsibilities for CIS support.
- Instructions pertaining to routine administrative and logistic support, including personnel policies and procedures, supply and maintenance procedures, inspection procedures, physical security, and other areas as directed by the unit commander.

Additional subjects to consider include specific responsibilities for sections and/or individuals as well as for subordinate units, guidance for inclusion in the SOPs of subordinate units, CIS policies, key references, exercise guidelines, safety instructions, and displacement procedures.

6402. CEOI

The CEOI contains the technical guidance required to establish and maintain communications support of operations. The CEOI amplifies the CIS SOP by providing detailed guidance for the coordination and control of communications means and functions. SPEED includes the Revised Battlefield Electronic CEOI System (RBECS), a module to support generation of the CEOI. Input is normally requested from subordinate commands by higher HQ. Sufficient copies of the CEOI should be maintained by the issuing HQ to allow issue to other units that may be attached for an operation. The following information and instructions can usually be included in the CEOI:

- Call sign assignments.
- Frequency assignments.
- Radio guard charts (app. M).
- Radio net identifiers.
- Telephone directory names and numbers.
- Identification and marking panel codes.
- Signal panel message instructions.
- Pyrotechnic and smoke codes.

- Ground-to-air signals.
- Sound warning signals.

6403. CIS Plan

A CIS plan is normally created by combining the CIS SOP and the CEOI. This combined document then becomes a basic CIS plan. The tactical and administrative instructions of the SOP form the body of this plan. The operating instructions of the CEOI are normally issued as a supplement. During the discussion of the tactical and administrative instructions in the body, reference should be made as necessary to the supplement that contains related technical operating instructions. The preparation of the operating instructions as a separate supplement facilitates revision or extraction as the need arises.

6404. CIS Estimate

As discussed earlier, the CIS estimate is a tool or procedure the G-6/S-6 uses to assist the commander in determining the best COA to accomplish a mission. On the basis of CIS estimates, the G-6/S-6 provides the commander with insights into the supportability of alternative COAs and recommendations on how available means can best support the selected COA. Appendix I provides a suggested format for the CIS estimate. The process of developing a CIS estimate is analogous to and completely integrated with the process of developing a preferred COA for the operation. Depending on the time available, several iterations may be performed as COAs are refined and modified, and the CIS estimate is updated accordingly. The following five steps are useful for preparing the estimate:

- Develop an understanding of the mission, the commander's intent, and the situation.
- Consider all factors that affect employing CIS, and develop alternative approaches to satisfy CIS requirements.
- Analyze each alternative to determine its advantages and disadvantages.

- Compare the alternatives and select the best one.
- Translate the selected solution into a decision (if the commander's estimate) or recommendation (if the G-6/S-6 estimate).

6405. CIS Concept

After developing the CIS estimate and gaining the commander's approval, the CISO prepares the CIS concept. The concept outlines how CIS are to be employed to support command and control throughout the operation. The CIS concept includes information such as—

- Numbers, types, classification levels, and locations of C2 facilities.
- Numbers, types, classification levels, locations, and mode of operation of SCR nets.
- Numbers, types, classification levels, locations, and channelization of MCR circuits, including location of transmission equipment.
- Numbers, types, classification levels, and locations of wire circuits, including location of terminal equipment.
- Numbers, types, classification levels, and locations of radio-wire integration facilities.
- Numbers, types, classification levels, and locations of LANs.
- Numbers, types, classification levels, and locations of switching centers, routers, and gateways.
- Numbers, types, classification levels, locations, and channelization of satellite links, including location of terminal equipment.
- Numbers, types, classification levels, and locations of terminal devices (computer, facsimile, etc.).
- Frequency requirements.
- Call sign requirements.
- Visual, sound, and messenger communications.
- Communications control procedures, including number, types, and location of communications control facilities.

The above list is not all-inclusive. It provides general guidance for preparing the CIS concept. Concept development should be closely coordinated with OPLAN/OPORD development. The concept is modified and refined as necessary and then promulgated as Annex K to the OPLAN/OPORD.

6406. Paragraph 5 of the OPLAN/OPORD

The culmination of all operational planning is the preparation and issuance of an OPLAN or OPORD. Information and instructions necessary to employ CIS and effect command and control are detailed in paragraph 5, Command and Signal, of the plan/order. As the member of the commander's general or executive staff with cognizance for employment of CIS in support of command and control, the G-6/S-6 is responsible for preparing paragraph 5. The G-6/S-6, with input from the G-3/S-3, will provide the draft paragraph 5 to the staff section with overall staff cognizance for the plan (G-5 at MEF level and above and G-3/S-3 at division/wing/FSSG level and below) or the order (G-3/S-3). See MCWP 5-1 (draft) for discussion on development of OPLANs/OPORD.

The command and signal paragraph covers several subjects: CIS establishment and maintenance instructions; CP location instructions; probable locations of future CPs; and command relationships. CP locations and command relationships information is provided by the G-3/S-3. Sections of paragraph 5 pertaining to the employment of CIS may consist simply of the notation "no change" if the existing CIS plan (CIS SOP and CEOI) is adequate for the operation. It may contain only changes or additions to an existing CIS plan/order if these are few. In either case, the existing CIS plan must be clearly referenced and available to all. Paragraph 5 will always include as subparagraphs *command relationships, signal, and CPs*.

a. Command Relationships

This subparagraph shows changes in or unusual command relationships. If there are none, the term "omitted" is used. For example—

- Command Relationships. Control of RLT-7 passes from 1st Marine Division to 2d Marine Division on order of CG, I MEF, on or about D+2.
- Command Relationships. Omitted.

b. Signal

This subparagraph references Annex K, the CIS Annex and other publications that are in effect, such as the CIS plan. It also includes instructions or restrictions pertaining to radio, visual, or sound signals. For example—

- Reference (b) (CIS plan) and Annex K (CIS Annex).
- Radio silence until lifted by this HQ.
- Signal for "assault waves have landed" will be green star cluster.

c. Command Posts

This subparagraph states the locations of the issuing unit's CP, subordinate unit CPs, and CP of the next higher unit. If an Annex K is not prepared, the CP locations of adjacent and supported units may also be shown to facilitate communication by messenger. In an amphibious operation, this subparagraph may also show CPs both afloat and ashore. This subparagraph should be considerably shortened by referencing CP locations on the operation overlay or, if one is prepared, in Annex K. This subparagraph may also direct subordinate units to report the location and opening/closing times of CPs. For example—

Command Posts

<u>Unit</u>	<u>Afloat</u> <u>(Ship Designation)</u>	<u>Ashore</u> <u>(Grid Coordinates)</u>
RLT 4	LHA	10268381
BLT 1/4	LPD	10254387
Co A	LSD	To be reported
Co B	LPD	10264391
Co C	LHA	18466832

Report initial location ashore and changes in location by priority message.

Additional subparagraphs may or may not be included. If used, they are lettered consecutively and may include the following information, as appropriate:

- Locations and times of opening/closing of C2 facilities.
- Use of CIS and equipment.
- Code words and names.
- Liaison procedures.
- Brevity List.

6407. Annex K (CIS Annex)

Annex K is an amplification of the instructions contained in paragraph 5 of the OPLAN or OPORD. It is a tool to coordinate the establishment, operation, and maintenance of CIS to support command and control. It delineates:

- The primary CIS missions to be accomplished by the organization.
- The CIS missions to be accomplished at the organizational HQ.
- The CIS missions assigned to subordinate units and (internal unit staff) principle staff officers
- Detailed technical plans for employment of CIS.
- Administrative and logistics details related to CIS.

In formulating an OPLAN or OPORD, MEFs, divisions, aircraft wings, FSSGs, and other major HQs normally find it necessary to issue a voluminous and detailed CIS Annex. However, the annexes developed by subordinate organizations are usually less detailed. The maintenance of a standing Annex K that can be tailored as necessary will greatly reduce the preparation time to develop a comprehensive Annex K for a specific operation. Furthermore, the Annex K should reference (or

modify) existing CIS SOPs and CEOI and not promulgate redundant information. Finally, by reference to the Annex K and/or the communications plan of a senior HQ, a subordinate organization may be able to place all necessary CIS instructions in paragraph 5 of its OPLAN, obviating the need to prepare a separate Annex K. However, there are still instances when the plan or order developed by a lower echelon should contain both paragraph 5 and a CIS Annex. For example, when a unit is involved in a highly complex operation requiring detailed CIS instructions to ensure that no salient points are omitted or misunderstood, such detailed instructions should be contained in a CIS Annex.

Annexes to an OPLAN or OPORD are prepared to—

- Promote clarity, brevity, and simplicity within the body of an order.
- Amplify parts of an order with data that is technical and/or limited in application to the command as a whole.
- Furnish guidance for development of a plan or order by a subordinate unit.

Annex K serves all three purposes. It amplifies paragraph 5 with data that is technical and, for the most part, limited in applicability, and at the same time eliminates the need for detailed CIS instructions in the main body. The CIS Annex also provides guidance to communications units for the development of their OPLANs and OPORDs. The G-6/S-6 should begin preparation of Annex K on the basis of the conclusions reached in the CIS estimate developed in support of the preferred COA and in close coordination with the overall development of the OPLAN or OPORD. Detailed instructions on the preparation of Annex K and a recommended format are contained in appendix J of this manual.

Section V

Communications Control

Communications control is the method used by the CISO to manage and provide positive control over the communications network and the employment of information systems. It involves organizing CIS personnel to plan, direct, and coordinate CIS support and controlling, engineering, installing, operating, and maintaining the MAGTF communications network. Communications control provides centralized control of limited CIS resources while allowing decentralized execution for greater flexibility and responsiveness. Communications control is the responsibility of the commander. The commander delegates this responsibility to the CISO, the G-6/S-6. The overall MAGTF communications control effort is the responsibility of the MAGTF G-6/S-6 officer. CISOs of subordinate organizations and units are responsible for providing communications control of the CIS resources of their respective organizations and units in accordance with the overall MAGTF communications control effort.

At the MEF, the G-6 exercises communications control with the assistance of a staff that is augmented by the supporting communications battalion. An MCCC is organized under the direction of the G-6. The MCCC directs both internal and external communications control functions. External communications control is coordinated with the JTF or CINC J-6 through the joint communications control center (JCCC). The functions and responsibilities of the JCCC are described in CJCSM 6231.01A, *Joint Tactical Systems Management*, and CJCSM 6231.07A. The MCCC also provides communications control support to the Marine component HQ.

Although communications control responsibilities, functions, and organization are more complex at higher echelons of the MAGTF, communications control is exercised throughout the MAGTF down to battalion/squadron level.

Many of the communications control functions supported by the communications battalions for the MEF and the Marine component are performed by the MWCS, the division and FSSG communications companies, and, at lower echelons, communications platoons and detachments. Likewise, many of these functions associated with SCI communications are performed by the radio battalions (for the MAGTF CE) or division and wing special security communications teams.

6501. Phases

Communications control begins with planning for an operation/exercise and continues throughout the deployment, installation, maintenance, and re-deployment phases.

a. Planning

This phase consists of both operational and technical planning. It culminates in the issue of a command element OPORD and a supporting communications unit OPORD. This phase is characterized by extensive coordination meetings between the supporting communications unit(s) and supported staff.

b. Deployment

During this phase, OPCON of the communications units and/or detachments is transferred to the supported CE. The CIS plan is refined through coordination among the supporting communications unit(s) and the supported G-6/S-6 staffs and key staff officers (e.g., the G-2/S-2 for intelligence CIS requirements, the fire support coordinator for fires CIS requirements, etc.). Limited execution is performed during this phase, including tracking message traffic and operating in-transit radio circuits, as required.

c. Installation

This phase begins with the ship-to-shore movement and reoccurs with subsequent CP and organizational displacements. Central coordination of multiple tasks is characteristic of this phase. Particular attention is paid to maintaining communications links external to the command element. SCR links are of highest priority.

d. Maintenance

This phase occurs as terminal systems and network circuits become operational. It is highlighted by a shift from SCR to SBB-based systems, including installation and operation of LANs and support of voice traffic and router and switch-based message and data traffic over MCR links. It is important to keep the SCR installation, operation, and maintenance efforts separate from efforts to install backbone systems. Otherwise the criticality of maintaining the SCR network can interfere with efforts to install the SBB. During this phase, communications planning is continual to modify and adapt communications networks as necessary to support maneuver and displacement.

e. Redeployment

This phase is highlighted by coordinated efforts to deactivate and pack up systems and equipment and by a transition to a simpler, less capable communications network while maintaining the required level of communications connectivity and information transfer capability. Communications support must remain effective and responsive throughout this phase.

6502. Responsibilities

Communications control is the method of organizing communications personnel and facilities to provide positive control of communications. It includes planning, organizing, directing, coordinating, controlling, and evaluating circuitry and equipment to ensure effective support of communications requirements. As the level of command increases, so does the complexity of communications control. Communications control responsibilities include—

- Planning, engineering, managing, coordinating, and controlling the MAGTF communications networks, both GENSER and SCI, including SCR, local area, and SBB networks, as well as maintaining connectivity to external networks.
- Identifying problems with the communications networks and coordinating and controlling efforts to restore, reconstruct, or reroute circuits to resolve problems.
- Frequency planning, allocation, management, and deconfliction.
- Managing COMSEC assets and monitoring compliance with COMSEC procedures.
- Managing, coordinating, and supervising tactical information systems employment in concert with principal staff officers representing functional area users.

6503. Functional Areas

Communications control is divided into the functional areas of system planning and engineering, SYSCON, and TECHCON.

System planning and engineering consists of determining the CIS requirements of the organization; designing the communications networks to support those requirements; and promulgating CIS plans, orders, and directives.

SYSCON consists of supervising, coordinating, and controlling the overall, day-to-day operation of MAGTF communications networks.

TECHCON consists of centralized technical supervision of the installation, operation, and maintenance of MAGTF communications networks. At the MEF and MSC level, a SYSCON staff and an OSCC support the SYSCON function, and a TECHCON operations staff and facility support the TECHCON function. Figure 6-1 is an overview of MEF communications control. Sections VI through VIII discuss these three functional areas and the specific responsibilities and tasks associated with performing them in support of MAGTF tactical communications networks.

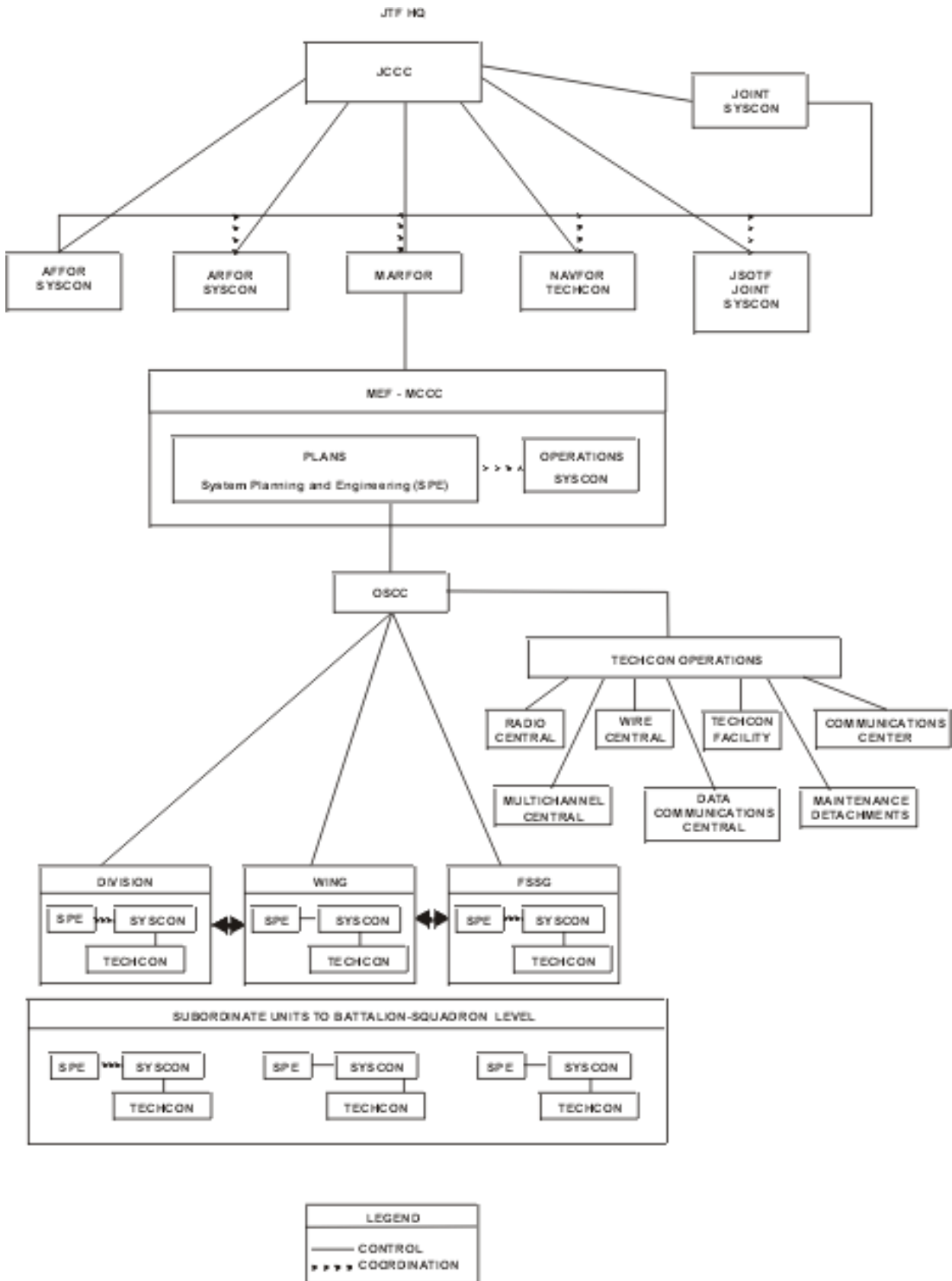


Figure 6-1. MEF Communications Control.

Section VI

System Planning and Engineering

System planning and engineering involves the technical aspects of designing the MAGTF tactical communications networks. These networks are planned, designed, and engineered to meet the operational requirements set by the CISO. The type and number of circuits required, circuit routes, frequency management, and other considerations are evaluated to establish requirements for both internal and external communications. System planning and engineering is performed by each CISO in the MAGTF. The MEF G-6 is the senior CISO and directs the overall system planning and engineering of CIS networks. The communication battalion provides personnel to support system planning and engineering at the MEF level. The CISOs at lower echelons plan communications support for their respective organizations in accordance with the overall MEF communications plan.

6601. Functions

System planning and engineering is conducted at all echelons and includes the following functions:

- Prepare and disseminate general command policies for the use of CIS within the command.
- Prepare and issue communications and information orders, records, and reports for the use of CIS and equipment within the command subordinate elements.
- Maintain continual contact with other staff elements to ensure awareness of the operational environment and evolving CIS requirements and coordination with the CIS staffs of other units in the AO.
- Specification of system interfaces to other-Ser-vice and joint networks and the DISN.
- Planning and engineering of the overall configuration of the command's communications networks, including the general locations of multichannel terminals, switches, gateways, cable routes, and LANs and the use of host nation

facilities, radio net structure, relay/retransmission sites, frequency requirements/allocations, and alternate means of communications.

- Analyzing the need for system reconfiguration and priority restructuring.
- Prepare and issue directives on implementing changes in network configuration, connectivity, or routing resulting from unit displacements, modifications of missions, unsatisfactory system performance, or other reasons.
- Continual review of system status and performance of communications equipment and personnel.
- Planning system expansion, extension, compression, or reconfiguration.
- Prepare and update contingency plans.
- Establishing network priorities.
- Monitoring progress of work implementation and quality assurance testing.
- Coordinating frequency requests and developing a frequency management plan that includes frequency allocation for both communications and noncommunications emitters such as radar.
- Maintenance of the system planning and engineering database.
- Prepare communications operations reports and maintain historical data and files.
- Inform the commander and staff of the communications situation.
- Prepare and plan COMSEC requirements (keys, codes, equipment, etc.) for the communications networks.
- Coordinate the development of automated tools to enhance system planning and engineering capabilities.

6602. Responsibilities

The MAGTF CISO is responsible for planning the SCR, local area, SBB, and special purpose system networks. Subparagraphs a–c address specific

system planning and engineering responsibilities with respect to each of the communications networks. Responsibilities for LANs are included under the SBB.

a. SCR

Planning SCR operations is the responsibility of CISOs at all MAGTF levels. Each level can employ a specific radio differently; however, interoperability and interference require consideration of factors such as frequency selection, cryptographic equipment, communications protocols, and frequency separation. SCR nets used by the MAGTF are described in appendix D.

(1) VHF and UHF Frequency Hopping Radio Networks. These networks include the SINCARS and HAVE QUICK radio systems. Both of these systems employ frequency hopping techniques. The set of frequencies, or hopset, to be used is planned and allocated by the MAGTF frequency manager. The MAGTF CISO assigns a unique net identifier to each net within the MAGTF. Current policy is for the net identifier to be permanently assigned in the MAGTF master net list. The MAGTF CISO identifies the MAGTF COMSEC keys for each net.

(2) Satellite Systems. The AN/PSC-5 is a single-channel UHF satellite radio system used for communication both within and external to the MAGTF. The area NCTAMS performs the link performance calculations, plans the uplink and downlink frequencies, and provides the satellite location information for antenna pointing calculations. When the radio is employed within the MAGTF, the MAGTF CISO identifies the COMSEC key to be used. If the radio is employed to communicate outside the MAGTF (JTF, other Services, and agencies), the higher HQ is responsible for security planning.

(3) HF Systems. Factors for HF communications interface planning include terminal selection, data rate selection, and operational mode. These are the responsibility of the MAGTF CISO. The MAGTF frequency manager is responsible for the propagation prediction. This includes calculating the maximum usable frequency, the low-

est usable frequency, and the frequency of optimum transmission for skywave propagation. The MAGTF frequency manager must then request frequency assignments from the area frequency coordinator. The power requirement and range for groundwave propagation are also responsibilities of the frequency manager. Additionally, the MAGTF CISO is responsible for identifying required COMSEC keys.

b. Switched Backbone

(1) Switching Systems. The MAGTF CISO is responsible for the detailed planning of the MAGTF SBB on the basis of user requirements. Each MSC CISO determines user requirements from within the command and forwards this information to the MAGTF CISO. On the basis of this information, the MAGTF CISO designs the network by establishing the trunking requirements from the MAGTF CE to each MSC and between the MSCs. From this design, each MSC CISO completes the detailed planning for the MSC switching system, including trunking to subordinate units, trunking between subordinate units, and loop termination assignments. The MAGTF CISO prepares and distributes the network timing plan to the subordinate units, indicating the master timing source for the network. From this overall plan, the unit CISO develops the internal site timing plans. The MAGTF CISO identifies the COMSEC keys for the MAGTF switched network and identifies the COMSEC and alternate COMSEC parent circuit switches.

(a) AN/TTC-42. The MEF employs AN/TTC-42 circuit switches at the MEF CE and at each MSC HQ. The MAGTF CISO, after consulting with the GBNP, determines the numbering scheme to be used and develops the circuit switch numbering plan. The MAGTF CISO also assigns telephone numbers and publishes the information systems directory (app. E). The interswitch trunking assignments and interoffice and interarea routing schemes are also the responsibility of the MAGTF CISO. Unit CISOs are responsible for configuring their switches to meet network design requirements and for providing subscriber service. Unit CISOs are also responsible for reporting their local plans and operational problems to

the MAGTF CISO. The MAGTF CISO determines the priority for restoration of service.

(b) SB-3865. The SB-3865 circuit switch is used throughout the MAGTF, within each MSC, and at subordinate units. It has operating characteristics similar to the AN/TTC-42. Therefore, the planning requirements, with minor exceptions, are the same as for the AN/TTC-42. The MAGTF CISO determines the priority for restoration of service. No planning is involved in selecting the number format because the SB-3865 accepts only the tactical numbering format (4/3).

(c) AN/MS-63A. The AN/MS-63A communications central is employed as a message switch at the MAGTF's CE and major subordinate elements. Connectivity for the AN/MS-63A is planned at two levels: the MAGTF CE level and the MSC level. When employing the AN/MS-63A, users must plan for communications connectivity because the AN/MS-63A does not have organic communications equipment. If GENSER and/or SCI communities are to be served, the users, inter-Service requirements, and security requirements must be identified.

(d) IP Routers. The Marine Corps employs IP routers to provide a data communications capability over the SBB and to interface with the SIPRNET, NIPRNET, and JWICS. The MAGTF CISO also has overall responsibility for network security on the SIPRNET. The MAGTF CISO coordinates with MSC CISOs to ensure router connectivity throughout the MAGTF. Communications and special communications units at the MAGTF CE and MSCs are responsible for the installation, operation, and maintenance of the MAGTF secure and nonsecure data networks. After the networks are operational, the communications unit monitors the network for activity, reliability, and security. Any detected security violations are reported immediately to the unit CISO and the unit security manager. See appendix M for an example of an IP network diagram.

(2) Transmission Systems. The MAGTF CISO is responsible for planning the systems for transmission from the CE to the MSCs and between

MSCs. Circuits that run from each MSC HQ to its subordinate units are the responsibility of the MSC CISO. If the MAGTF uses external means to communicate outside of the MAGTF (JTF, other Services, and agencies), the planning requirements are coordinated with the higher HQ. The following transmission systems employment considerations provide some understanding of the CISO's responsibilities.

(a) CX-4566, 26-Pair Cable. CX-4566 is used to extend the distance of subscriber terminal equipment from assemblages and switches and to perform the function of a link concentrator when used with a J-1077 junction box.

(b) CX-11230, Coaxial Cable. The CX-11230 provides the connectivity between switches, switches and transmission systems, and data terminals.

(c) Fiber-Optic Cable System. The fiber-optic cable system provides the connectivity from the switch equipment to the transmission equipment or between switches.

(d) AN/MRC-142. The AN/MRC-142 is a UHF transmission system employed by each MSC within the MAGTF. This system provides critical line-of-sight communications from the MAGTF CE to the HQs of subordinate commands, between MSC HQs, and within each MSC. The AN/MRC-142 baseband configuration is planned by the MAGTF CISO with input from the MSC CISO. Profiling and frequency planning between the CE and MSCs and between MSCs are accomplished by the MAGTF CISO. Systems internal to an MSC are profiled by the MSC CISO. Site selection and antenna elevation are the responsibility of the CISO employing the equipment and are based on the profile of the system.

(e) AN/TRC-170. The AN/TRC-170 radio terminal set is used for line-of-sight or troposcatter communications by the MEF CE, each MSC within the MEF, and between elements of the ACE. The MAGTF CISO, with input from the MSC CISOs, coordinates baseband configuration and profiling of the AN/TRC-170s between the CE and MSCs and between MSCs. The MAGTF CISO is

responsible for the frequency planning for the AN/TRC-170 systems.

(f) AN/TSC-85B and AN/TSC-93B. These terminals provide entry into the GMF satellite system and the DISN gateway. The MAGTF CISO plans for employing the AN/TSC-85B satellite terminal at the CE. At the MSC locations, the MSC CISO plans for employing the AN/TSC-93B. The baseband configurations of the AN/TSC-85B and AN/TSC-93B are planned by the MAGTF CISO in coordination with the MSC CISOs. The MAGTF CISO submits a satellite access request to the Regional Space Support Center in CONUS, Europe, or the Pacific for entry to the GMF satellite system. The Regional Space Support Center will produce and provide a satellite engineering plan that includes the path, link analysis, uplink and downlink frequencies, azimuth and elevation for the antenna, and satellite assignments. The results are sent to the MAGTF CISO and then to the MSCs for employment of the GMF equipment.

(g) AN/TSC-96A. The AN/TSC-96A is a UHF satellite communications system designed to work with the Fleet Satellite Communications (FLT-SATCOM) network. It is employed down to the MSC level within the MEF. The baseband configuration of the AN/TSC-96A is planned by CISOs of the MSC. Because this is a satellite system, the link performance calculations, uplink and downlink frequencies, and the antenna pointing calculations are planned by the NCTAMS servicing the AO. A communications information bulletin is published by the area NCTAMS. The communications information bulletin provides the satellite coverage of the area, base frequencies for reestablishment of links, and the types of information transmitted over each satellite channel. There is a communications information bulletin published for each operational area of the world. MEF and MSC CISOs should request copies of the communications information bulletin before they deploy. The COMSEC keys to be used with this system are planned by the parent agency of the system.

(h) AN/TSC-120. The AN/TSC-120 is employed at the MEF and MSC HQs and provides internal and external communications. It can operate with both U.S. and NATO conventional and special opera-

tions forces. The CISOs at each echelon plan for the employment of the AN/TSC-120 and are responsible for the proper employment of the system, including terminal equipment selection, data rate selection, and mode of operation. The CISOs also submit communication guard shifts to ensure system entry into the Naval Telecommunications System and DISN.

When employing this system, the MAGTF CISO and frequency manager must confirm the availability and allocation of multiple frequencies necessary for effective operation and circuit reliability. Calculation of skywave propagation parameters is also required. In addition, power requirements and range for groundwave propagation employment must be considered. The area NCTAMS performs the link performance calculations for the AN/PSC-5 employed with the TSC-120, plans the uplink and downlink frequencies, and provides the satellite location information for antenna pointing calculations. The MAGTF CISO is responsible for planning power requirements, range, and message throughput and wait times for VHF-AM meteor burst employment. When the AN/TSC-120 is employed within the MAGTF, the MAGTF CISO identifies the COMSEC key to be used. If it is employed to communicate outside the MAGTF (JTF, other Services, and agencies), the higher HQ is responsible for security planning.

(3) Special-Purpose Systems

(a) PLRS. The PLRS is a ground-based radio-navigation system. Employment of PLRS is the joint responsibility of the GCE operations and CIS officers and the MAGTF CISO. The GCE operations officer is responsible for operational planning, including basic user unit equipment distribution, group access, message set access, and navigational aids (zone, corridor, and line boundaries and predetermined items). The MAGTF CISO is responsible for planning the initial locations of the PLRS master station and alternate master station. The GCE operations officer determines the organizations that will provide the necessary 6–10 reference units and coordinates with the CISO for their initial locations. The MAGTF CISO is responsible for planning reference units and coordinates with the GCE CISO for their initial

locations. The MAGTF CISO is responsible for planning reference and relay unit locations to ensure complete PLRS coverage. The MAGTF frequency manager provides the net frequency allocation and a single-channel VHF frequency for the PLRS engineering net. In the event that more than one PLRS network is operated, the MAGTF frequency manager plans for additional frequency allocations for the additional networks.

(b) EPLRS. EPLRS employment requires detailed planning so that it can support the operational scheme of maneuver. All predetermined EPLRS data communications needlines must be planned and established prior to mission execution. Continuous coordination between the operations officer and communication-electronics officer of operational headquarters throughout the MAGTF is necessary for effective employment of EPLRS. EPLRS network planning with consideration for TDN, DACT, TCO, AFATDS, and SINCGARS, and the cryptological key management plan are key mission planning factors. Additionally, for joint operations, coordination with Army EPLRS planners, Air Force Situation Awareness Data Link (SADL) planners, and Navy AN/KSQ-1 planners may be necessary.

During operations ashore, EPLRS will serve as the primary data radio set for TDN connectivity below the regimental level, as well as providing data communications requirements for task organizations below the battalion level. The network can be generated and established by an NCS-E(D) or a PC, dependent upon the particular mission. (The PC-based capability, *currently under development*, will be used for rapid communications network initialization, and generation of initialization and cryptographic keys to support garrison and field exercises, EPLRS radio set training, and host system training. This precludes deployment of an NCS-E(D) to support limited training environments and small operational deployments which do not require an automated PLI capability, but do require EPLRS data communications capabilities.)

If EPLRS and PLRS are also employed for PLI, the NCS-E(D) is required and will be located in the vicinity of the senior headquarters of the oper-

ating force. The tactical situation will determine its exact location. However, in making this determination, the commander should consider the scheme of maneuver, security requirements, EPLRS network requirements, and electromagnetic interference. The reference community can be based on a mix of fixed reference sites and radio sets with Global Positioning System Interface Units (GPSIUs). The GPSIU allows the employment of a mobile, more versatile reference community, vice fixed reference units which must be surveyed, by connecting an organic AN/PSN-11 PLGR to either an EPLRS radio set or PLRS BUU. A single EPLRS/PLRS community will be deployed with one NCS-E(D) and up to 460 active radio sets.

During ship-to-shore movements, the Marine Corps EPLRS network can be integrated with the U.S. Navy's Amphibious Assault Direction System (AN/KSQ-1). (Net Control Stations are being installed on all LHAs and LHDs as part of this system.) The AN/KSQ-1 is designed to monitor and control naval surface landing craft—LCUs and LCACs—as well as “inject” PLI generated by these craft into the Joint Maritime Command Information System (JMCIS) Track Database Manager (TDBM) for building the common operational picture. Airborne or terrestrial platforms equipped with EPLRS can provide “over-the-horizon” communications, dependent upon the mission and platform availability. In order to capitalize on EPLRS communication and PLI capabilities, extensive coordination and planning must be done in order to establish and manage the data needlines for Marine and Navy use.

(c) JTIDS. JTIDS is an airspace C2 support system. The TAOC and the TACC are the only Marine Corps C2 facilities to be equipped with JTIDS. The ACE CISO is responsible for planning implementation of the JTIDS terminals located within the ACE. The ACE CISO requests the required frequencies and time slots from the MAGTF CISO, who forwards the request to the JTF J-6. The MAGTF CISO is also responsible for identifying COMSEC key requirements. The JTF J-6 assigns the frequencies to be included in the frequency allocation and the time slots for operation in the network. The ACE CISO coordinates with the ACE operations officer to

determine the locations of the JTIDS modules associated with the TAOC and TACC.

(d) GPS. The GPS is a passive system, and there are no communications networks for the MAGTF CISO to coordinate. However, the MAGTF CISO must ensure that satellite coverage is available in the AO. This information is found in the satellite almanac published by the U.S. Air Force Space Command. The data in the almanac includes the number of satellites covering the AO, the actual number of satellites operating, and the times the satellites are overhead. The GPS satellite almanac data is also transmitted automatically to GPS receivers from the GPS satellite constellation.

(e) Trojan Spirit II. Each day, a portion of the radio electronic spectrum is captured by selected SIGINT collection facilities overseas and relayed via the Trojan Spirit intelligence support system to CONUS-based analysts for further exploitation. Trojan Spirit (fig. 6-2) is a unique transmission capability designed to forward tactical SIGINT to CONUS-based elements for analysis. Operating at the SCI/TK level, the Trojan Spirit system is fielded and operational in the MEFs. Operators at the Intelligence Company of the MEF, in conjunc-

tion with analysts from Radio Battalion, can receive live SIGINT information being collected in the forward area. This capability enables analysts to train and maintain their readiness in collection management, technical control, and system supervision, as well as SIGINT production and data base maintenance.

The executive authority for Trojan Spirit is the U.S. Army Intelligence and Security Command (INSCOM) at Fort Belvoir, VA; management is provided by the U.S. Army Technical Control and Analysis Element (TCAE) at Fort Meade, MD. Use and management of the Trojan Spirit system is exercised at Fort McPherson, GA. Trojan Spirit services are extended to the I, II, and III MEFs.

In addition to supporting the counter-drug mission, language training, an essential element of the intelligence training program, is a secondary purpose of the system. The command provides secure facilities and communications with intelligence staff oversight and INSCOM technical control for the training of SIGINT skills, tasks, and processing of assigned units under TCAE operational control.

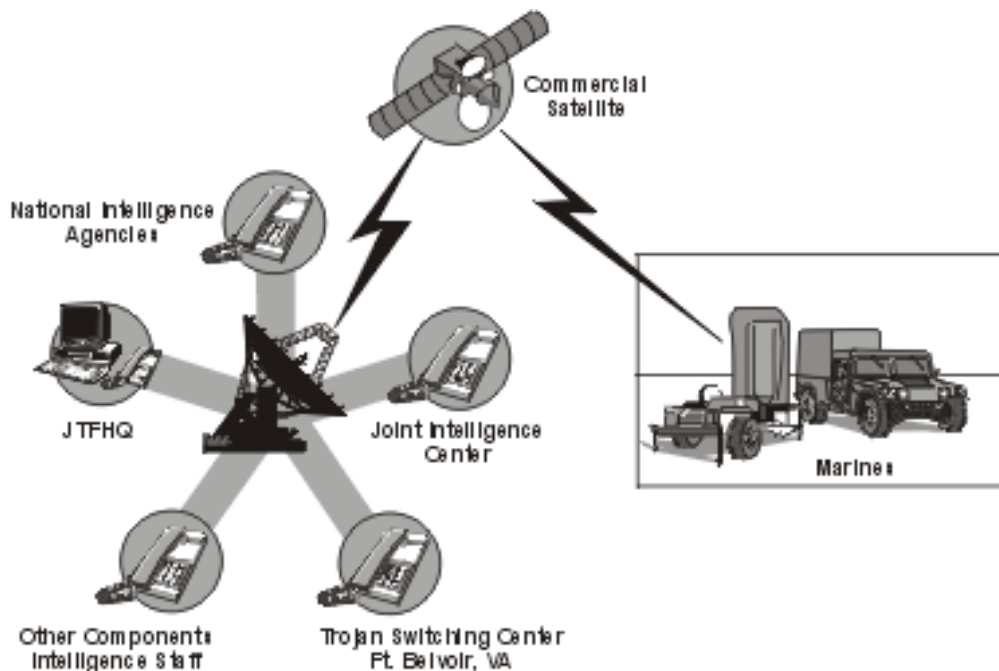


Figure 6-2. Trojan Spirit.

The Trojan Spirit system consists of four major elements: the remote collection equipment in the forward area, transmission systems that carry the actual transmission to CONUS, central switching facilities at Fort Belvoir that route traffic to specific processing sites, and the garrison central operating facility.

A basic Trojan Spirit system consists of four collection positions, four listening posts, a system supervisor's console, and system-associated communications equipment. An upgraded capability includes enhanced signal distribution interconnecting control and digital data switching. The tactical field monitor sub-component of the Trojan Spirit system is designated the AN/TSQ-144(V)2. This equipment can remotely control receivers at unmanned collection sites. From the collection site, secure communications links are established using tactical military equipment such as SHF/GMF terminals employing the DSCS, most often a combination of U.S. military-owned/-leased commercial connectivity using satellite and terrestrial systems.

Although Trojan Spirit is oriented toward CONUS garrison operations, the system has tactical applications, as was proven during Operations Desert Shield/Desert Storm. The Army realized that it had a robust wide-band communications asset that could be used to support tactical operations. During Operation Restore Hope, using Trojan Spirit to support split-based operations reduced the number of intelligence personnel required to deploy.

Future TS IIs will provide MEFs with both C- and Ku-band satellite communications; planned fielding will remain at two systems per MEF. The HM-MWVs are currently configured with a primary Trojan shelter on one vehicle and a spare equipment shelter on the other. Both vehicles have under-the-hood and tunnel-mounted electrical power generating capabilities. The space between the HMMWV cab and the shelter contains the tunnel-mounted generator. The system also has a mobile antenna platform trailer.

6603. Automated Tools

Several automated planning and engineering tools are available to support system planning and engineering.

a. SPEED

SPEED is a team-transportable, fully integrated, microcomputer-based system that supports MAGTF tactical communications planning to the regimental/group level. SPEED is used in conjunction with a random data generator and a data transfer device. SPEED should have other programs which provide the following capabilities:

- Point-to-point analysis.
- High-frequency analysis.
- Guard chart application.
- Signal/noise and signal/interference analysis.
- Area coverage analysis.
- Topographic database.
- Database of basic equipment characteristics.
- RBECS software programs for CEOI/signal operating instructions generation.
- Tactical Network Analysis and Planning System Plus (TNAPS+) software.
- Switched Network Automated Planner software.

b. Revised Battlefield Electronic CEOI System

RBECS application software was designed to provide the user with an enhanced CEOI and frequency hopping data generation capability. RBECS is one of the applications resident on SPEED terminals. There are two application modules within RBECS: Signal operating instructions/CEOI and Revised SINCGARS Integrated Communications Security Module, Nonintegrated Communications Security Module Support Software (RSI-NISS). Signal operating instructions/CEOI provide the user with the capability to build, generate, edit, and print CEOI locally for training or operations. CEOI generation requires an AN/CSZ-9 random data generator and is conducted at the MEF, MSC, and MEU CE levels.

c. Revised SINCGARS Integrated Communications Security Module, Nonintegrated Communications Security Module Support Software

This application of the RBECS was designed to generate, store, edit, and transfer SINCGARS frequency hopping data. RSINISS can download frequency hopping data from a PC into a DTD by using RS-232 cable or to a floppy disk for dissemination to subordinate, adjacent, or supporting units. RSINISS requires a random data generator to generate unique transmission security keys. Transmission security keys are generated at the MEF, MSC, and MEU CE levels.

d. AN/CSZ-9 Random Data Generator

The random data generator performs two basic functions. It randomizes the allocated frequencies into daily changing frequencies and assigns daily changing call signs for the CEOI application. It generates a unique pseudo random transmission security key for RSINISS use when creating load-sets.

e. AN/CYZ-10 DTD

The DTD is a weather-resistant, electronic data storage and transfer device procured by the National Security Agency loaded with RBECS DTD Software. The DTD is cargo-pocket size, weighs 1.5 pounds, and requires three 3-volt batteries or one 9-volt battery. DTD's primary function is to serve as a common fill device to load COMSEC keys into any Marine Corps cryptographic equipment. It is the planned replacement for the TSEC/KYK-13 and the TSEC/KYX-15. The DTD can receive, store, and transfer frequency hopping data between DTDs or PCs. The DTD can also receive, store, display, and edit CEOI information and transfer one time period of CEOI information over the air by using a SINCGARS radio. The DTD is also referred to as the Automated Net Control Device (ANCD) in many U.S. Army technical and operation manuals.

f. Revised Battlefield Electronic CEOI System DTD Software

This is the software application used by the Army and Marine Corps in the DTD. RBECS DTD

Software has two application modules: signal operating instructions and radio. Signal operating instructions can receive, store, find, display, and transfer CEOI data. Radio can receive, store, edit, and transfer frequency hopping data. Radio can also generate, receive, store, and transfer COMSEC keys.

g. ARC-210 Fill Program

The ARC-210 Fill Program is a software application located on the SPEED platform. The ARC-210 Fill Program is used to enter and organize the various types of data required to fill an AN/ARC-210 radio: single-channel frequencies and related data and HAVE QUICK and SINCGARS frequency hopping data. This data allows the radio to operate in either single-frequency or frequency hopping modes with compatible radios.

h. Consolidated SCR EP Package

The Consolidated SCR EP Package is a software application that may be loaded into the DTD. The Consolidated SCR EP Package allows the DTD to receive frequency hopping data from RSINISS and COMSEC keys from common fill devices. The Consolidated SCR EP Package application consists of two functions: detailed management and quick fill. The detailed management function offers transmit, receive, database, and setup functions. The quick fill function transfers frequency hopping data from the DTD to a SINCGARS or AN/ARC-210.

i. TNAPS

TNAPS is a computer-based desktop system planning and SYSCON tool that assists the planner in building an exercise or operation database and in producing a series of output reports describing the resulting networks and equipment configurations. The system controller can use this database with program support to monitor and manage in-place communications. TNAPS allows tactical communications planning and control at two levels: the network level and nodal/equipment level. Network planners and controllers are responsible for planning and managing the overall network. Nodal planners and controllers plan and manage a complete database for equipment within the node

and generate all necessary worksheets and crew assignment sheets. Some of the functions of TNAPS are—

- Exercise of database control.
- Site configuration and inventory control.
- Circuit/message switch graphics and network development.
- Transmission graphics and network development.
- COMSEC database control.
- Report generation.

- Subscriber database control.
- SYSCON.

j. Switched Network Automated Planner

The Switched Network Automated Planner is used to plan and engineer switched communications networks. Through a series of user selections and inputs and software routines, the Switched Network Automated Planner assists in planning and engineering a network and provides physical and database configuration data for ULCS equipment.

Section VII

SYSCON

The primary purpose of SYSCON is to ensure optimum use of all available circuits to meet the requirements of the commander. SYSCON is the responsibility of the supporting communications unit. The SYSCON function includes two types of activity: staff direction of MAGTF communications network configurations and day-to-day management of the operating communications networks. These functions are accomplished by the SYSCON staff and the OSCC watchstanders, respectively. The SYSCON staff supervises OSCC activities and compiles statistics and reports for use in long-range planning. The OSCC meanwhile directs day-to-day operations of the communications networks within the MEF. The communications battalion provides the SYSCON staff and mans the MEF OSCC. At the MSC level, the supporting communications unit(s) provide the same functions. At lower echelons, SYSCON functions are less complex and are performed by personnel of the communications unit without establishment of an OSCC.

6701. Functions

The SYSCON functions performed by the SYSCON staff and the OSCC are—

- Prepare and issue detailed directives and instructions to subordinate communications units for implementation of CIS plans and supervising the execution of the plans.
- Monitor system performance and coordinate actions required for restoration of system outages, including coordination with senior, subordinate, and adjacent OSCCs.
- Generate and disseminate frequency assignments and monitor and control frequency usage.
- Maintain the transmission quality on all transmission links.
- Adjust communications resources to compensate for disruptions or destruction of the communications system by the enemy.

- Achieve speed and grade-of-service goals in the network under normal and stress conditions.
- Determine satellite/transponder usage and monitor the channels for occupancy to determine whether a reallocation of channels is necessary.
- Provide circuit switch, message switch, and router programming needed to establish and update subscribers and route traffic.
- Develop, monitor, and load key variables into encryption devices.
- Collect and analyze traffic data, service complaints, and outage reports to identify and correct system inadequacies, procedural deficiencies, and other problems and provide the analyses to system planning and engineering. Make recommendations to system planning and engineering for corrective actions when the resources available to SYSCON are insufficient to provide satisfactory communications service.
- Prepare and distribute information essential to using and operating the system, such as telephone directories, network addresses, and call signs.
- Maintain system records and historical data and submit reports as required.
- Direct and receive circuit information from the local TECHCON operations center.

6702. Staff Responsibilities

Communications, as a function of the command, are the ultimate responsibility of the commander. The CISO and the supporting communications unit operations officer act as agents of the commander. For example, the MEF communications battalion operations officer may provide direction to the division communications company operations officer. However, the division communications company operations officer is ultimately responsible to the division commander and serves as the agent of the division commander to express

the division communications requirements to the MEF.

At each echelon, the communications unit operations officer has been delegated the management and control responsibility necessary to direct the operation of the communications systems and networks. At the MAGTF CE, the communications unit operations officer is responsible for the communications links connecting the CE to the subordinate HQ. Directives from the MAGTF CISO are distributed down to each subordinate communications unit operations officer. The MAGTF communications unit operations officer periodically monitors the status of each link of the MAGTF communications networks, including equipment status. Reports from subordinate communications unit operations officers are consolidated by the MAGTF communications unit operations officer. Each subordinate communications unit operations officer monitors the equipment and network status within the command and reports the status to the MAGTF communications unit operations officer. For systems between adjacent subordinate HQs (e.g., GCE to ACE), the MAGTF CISO designates one of the subordinate communications unit operations officers to control the link.

a. SCR

Each subordinate communications unit operations officer or commander monitors the status of SCR nets and provides periodic status reports to the next higher command communications unit operations officer. If an MSC communications unit operations officer is notified of a COMSEC or TRANSEC compromise, the MAGTF CISO is informed. Each subordinate communications unit operations officer informs the next higher communications unit operations officer of any interference problems that require additional frequency planning for HF, VHF, UHF, and UHF-SATCOM nets.

b. Switched Backbone

Each subordinate communications unit operations officer is responsible for directing the implementation of the SBB network according to plans developed or approved by the MAGTF CISO. The subordinate communications unit operations of-

ficers coordinate with adjacent units to resolve problems. Subordinate communications unit operations officers are responsible for providing periodic status reports to the next higher echelon. The MAGTF CISO is kept informed of the MAGTF communications network status by the MAGTF communications unit operations officer. Subordinate communications unit operations officers are responsible for reporting problems that cannot be solved at their level to the next higher communications unit operations officer.

c. Special Purpose Systems

Direction, management, and control responsibilities for special purpose systems consist primarily of reporting equipment status and outages. Status reporting for these systems is the same as described above for the switched backbone. Outage reports are sent to the external supporting organizations for these networks through the MAGTF CISO. Planning to circumvent outages is coordinated with the communications unit operations officer. The communications unit operations officer coordinates with the appropriate network organizations for access according to local SOP guidelines.

The MAGTF communications unit operations officer is responsible for directing, managing, and controlling the PLRS (EPLRS). The MAGTF communications unit operations officer directs the activities of the PLRS (EPLRS) master station operators in implementing OPLANs and plan changes. The PLRS (EPLRS) master station operators are responsible for the PLRS TECHCON functions. The MAGTF communications unit operations officer monitors the PLRS (EPLRS) network to check for full area coverage. If the area coverage is insufficient, the MAGTF communications unit operations officer notifies the MAGTF CISO. PLRS (EPLRS) employment must be integrated into the commander's scheme of maneuver and support execution. This means that the network must be flexible and able to adapt to change as it occurs during all phases of planning and operations.

The MWCS operations officer is responsible for the SYSCON of the JTIDS. The MWCS

operations officer receives system status reports from the wing OSCC and reports system failures, frequency interference problems, and ground station movements to the wing CISO.

The MAGTF communications unit operations officer needs to ensure that the appropriate COMSEC variables are distributed so that encrypted positioning signals can be properly received. The MAGTF CISO monitors almanac conditions, coordinates appropriate adjustments, and forwards information messages to GPS users. System outages are reported to U.S. Air Force Space Command.

6703. OSCC Responsibilities

The OSCC directs the day-to-day operation of communications networks.

a. SCR

The OSCC directs the implementation of the SCR nets, including coordination with the unit operations section for the operation of the net control station. The OSCC also maintains the COMSEC and TRANSEC keys, the word of the day, and the net frequency allocation for each net. The TECHCON of the tactical radio nets, including troubleshooting, is directed by the OSCC. To combat interference or to limit the amount of traffic on a net, the OSCC and the operations officer may decide in favor of time sharing of nets or directed net operations. The OSCC periodically reports the tactical radio net status to the communications unit operations officer.

b. Switched Backbone

The OSCC maintains the equipment status of each system. The OSCC also monitors the circuit switched network statistics to insure that system availability, call blocking, and the switch traffic load are within acceptable tolerances. The OSCC directs the installation of the switch network to include fault isolation, restoration, and reconfiguration, as necessary. The OSCC institutes preauthorized changes in the switched network such as routing table changes, zone restrictions, alternate routing, database changes, or traffic load

control procedures. The OSCC reports problems that cannot be resolved at that level to the respective communications unit operations officer. The OSCC is also responsible for directing the loading of the proper COMSEC keys into the equipment and ensuring proper operation. The OSCC compiles the statistics of the switched network and reports them to the communications unit operations officer.

c. Special Purpose Systems

The primary functions of each OSCC are to direct the installation of the systems, maintain the equipment status, and report equipment outages to the communications unit operations officer. Security management is also the responsibility of the OSCC. The OSCC provides COMSEC keys and ensures proper operation.

The majority of PLRS (EPLRS) OSCC duties, such as monitoring reference units and coordinating with multiple network PLRS (EPLRS) master station operators, must be done at the master station location. The PLRS (EPLRS) master station operator is responsible for fulfilling the duties of the OSCC. The master station operators are responsible for reporting the status of the network to the MAGTF communications unit operations officer. They also provide the COMSEC keys to the necessary personnel. The master station operators continually monitor the units that are active users of the PLRS (EPLRS). Units moving out of the area of coverage are reported to the communications unit operations officer for action. Master station operators are also responsible for verifying the map, control, and coordination data that appears on the monitors.

The ACE OSCC directs the JTIDS installation, operation, and maintenance; provides the COMSEC key to the JTIDS operators; and coordinates the movement of the JTIDS ground stations. The OSCC provides system status, frequency interference, and ground station movement reports to the communications unit operations officer.

The MEF OSCC distributes COMSEC keys and information messages to GPS users.

Section VIII

TECHCON

TECHCON is the means of exercising centralized technical supervision over the installation, operation, and maintenance of the circuits and systems employed by the MAGTF. The installation of each system is controlled by a TECHCON facility. This includes both the systems that interface directly with the facility and those that do not. The OSCC watch officer directs the activities of the TECHCON operations staff. The TECHCON operations staff supervises the installation, operation, and maintenance activities of the direct support, general support, and service companies and/or their detachments. The capabilities of these units are organized around platoons and sections into centers such as radio, wire, multichannel, and data communications central; the TECHCON facility; the communications center; and the maintenance facilities. TECHCON operations staff oversees and directs the activities of all these centers.

6801. Functions

TECHCON functions are—

- Exercise technical coordination between elements of the MAGTF tactical communications network.
- Exercise technical supervision over subordinate technical control facilities
- Restore disrupted service.
- Perform quality checks and exercise technical direction, coordination, and supervision on system testing.
- Coordinate system activation, deactivation, and/or reconfiguration.
- Report system and circuit status to the appropriate control facility.
- Record status of transmission links, trunks, channels, and circuits as required by local SOP.

6802. Responsibilities

The current generation of digital switching and transmission equipment has been designed with inherent TECHCON capability. Because many of the component systems that make up the communications networks are physically isolated from one another, responsibility for the TECHCON of the communications networks involves the combined and coordinated effort of each operator, supervisor, and maintainer in each part of the system.

a. SCR

The responsibility for TECHCON of MAGTF tactical radio nets lies with the net control station equipment operators and the local communications organization. For frequency hopping radio nets to operate properly, each radio in the net must maintain an accurate time-of-day clock. The net control station maintains time of day and provides it to the users of the net. The equipment operators are responsible for maintaining synchronization within the network and correcting as necessary. Troubleshooting tactical radio nets is the responsibility of the local communications organization. The local communications organization also determines the separation and placement of antennas to minimize electromagnetic interference. The OSCCs direct equipment operators on the power setting that will allow them to operate in the net without using an excess amount of power.

b. Switched Backbone

The TECHCON for the SBB is accomplished by the operators and supervisors of the switch and transmission equipment, as well as by dedicated TECHCON personnel. The switch and transmission equipment operators are responsible for installing the individual circuits in the switched network and for monitoring the equipment

alarms. It is also the responsibility of the equipment operators to monitor the synchronization of the switched network. When circuit or system outages occur, the operators are responsible for notifying the OSCC and implementing procedures for fault isolation and restoring the lost service. If necessary, they reconfigure the circuits or systems under the direction of the OSCC. Equipment and circuit outages are reported to OSCC by the operators. Equipment operators are also responsible for monitoring and adjusting circuits that require alignment, such as analog voice and data circuits. The operators are also responsible for monitoring the status of each circuit and system and periodically reporting this status to the OSCC. In addition, there may be dedicated circuits installed that use the transmission systems but do not access the switched network. The TECHCON for these circuits may be accomplished by using portable TECHCON facilities that do not interface with other systems.

The current TECHCON facility is the AN/TSQ-84, an analog facility with limited capabilities. The digital technical control (DTC) is replacing the AN/TSQ-84. The DTC provides the FMF with a deployable, digital technical control capability to replace the AN/TSQ-84. The DTC facilitates the installation, operation, restoration, and management of individual circuits and digital links consisting of many multiplexed circuits. It provides the primary interface between subscriber systems/networks within a local area and long haul multi-channel transmission systems to transport voice, message, data, and imagery traffic. It can add, drop, and insert digital circuits into multiplexed groups; provide a source of stable timing

to connected equipment; condition circuits; and perform analog/digital, 2-wire/4-wire, and signaling conversions. It contains the monitoring, testing, and patching equipment required by technical controllers to troubleshoot and restore faulty circuits and links. Equipment is contained in an S-280 shelter and will be transported by a dedicated 5-ton truck. A total of 31 systems are planned for fielding to the FMF.

c. Special Purpose Systems

Because the special purpose systems are separate from the other systems within the MAGTF, the TECHCON is accomplished by the equipment operators. The operators monitor the status of the transmission and subscriber equipment. Reports of system status and outages are sent to the OSCC.

The PLRS (EPLRS) master station operators are responsible for the TECHCON duties. These responsibilities have been discussed in the day-to-day OSCC responsibilities.

The JTIDS operators at the TAOC and TACC perform the TECHCON functions for the JTIDS system. The JTIDS operators install and restore the JTIDS system under the direction of the ACE OSCC and report equipment outages and periodic system status to the ACE OSCC.

The MAGTF G-6 staff monitors almanac conditions and coordinates appropriate adjustments and information messages to GPS users. System outages are reported to U.S. Air Force Space Command.

Chapter 7

Information Systems Security

MAGTF command and control relies on the confidentiality, availability, and integrity of tactical communications networks and information systems. Protecting these systems from exploitation, disruption, or destruction is of highest priority.

The threat to MAGTF CIS comes from a variety of sources and continues to evolve. This threat ranges from conventional EW/SIGINT techniques to newer forms such as computer intrusions by hackers; drug traffickers; foreign intelligence agencies; disaffected, disgruntled, or disloyal personnel; and, potentially, battlefield adversaries. Intruders have repeatedly demonstrated their ability to penetrate military information systems. With the increasing interconnection of information systems, such attacks threaten the entire DII as well as the tactical communications networks and information systems that interface with and use that infrastructure.

INFOSEC is the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users or the provision of ser-

vice to unauthorized users, including those measures necessary to detect, document, and counter such threats.

As with other forms of security, the first step in providing effective INFOSEC is understanding the threat. This includes identifying threat objectives, capabilities, and techniques as well as friendly vulnerabilities.

The threat's overall capability to conduct C2 warfare on the battlefield and information warfare in the strategic arena affects the way the MAGTF must defend its information systems.

At the strategic level, DISA is responding to the threat with a defensive information warfare strategy based on protecting the infrastructure and data, detecting attacks, reacting promptly to attacks, and maintaining service. On the battlefield, the MAGTF is responding to the threat through a similar C2 protection strategy.

This chapter focuses on two key security disciplines: COMSEC and computer security (COMPUSEC).

Section I

Communications Security

COMSEC is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications or to mislead unauthorized persons in their interpretation of the results of such possession and study. COMSEC includes physical, cryptographic, transmission, and emission security. The goal of COMSEC is to protect friendly communica-

tions from enemy exploitation while ensuring unimpeded use of the electromagnetic spectrum. The organization must be able to employ communications equipment effectively in the face of enemy efforts. COMSEC is an integral part of electronic protection—the element of EW that focuses on protection of our capabilities. COMSEC requirements must be integrated into communications systems planning and must focus on provid-

ing secure communications without impairing reliability or responsiveness. Modern communications equipment includes features such as integrated encryption capability and frequency hopping capability, which contribute to communications protection. However, the security of our communications depends on the proper operation of communications equipment and adherence to proper procedures.

7101. Responsibilities

COMSEC is a command responsibility. It is also the responsibility of each individual user of communications. The G-6/S-6 is responsible to the commander for the overall planning, supervision, and coordination of COMSEC matters, including the administrative, day-to-day management of COMSEC material. Specific staff responsibilities include:

a. G-6/S-6

- Incorporating COMSEC requirements into the communications plan.
- Supervising communications to ensure proper equipment operation and use of COMSEC procedures.
- Training communications personnel in COMSEC and electronic protection techniques.
- Promoting awareness of the enemy EW threat among all members of the command.
- Advising and assisting the unit security manager, G-2/S-2, and G-3/S-3 in matters regarding CIS and electronic security and protection.
- Preparing an emission control (EMCON) plan to include employment of alternate communications means.
- Advising and assisting the G-3/S-3 in matters regarding the command's operations security and deception plan.
- Instructing all users on proper operation of communications systems and equipment and proper communications procedures.
- Coordinating with the G-2/S-2 and G-3/S-3 for conducting COMSEC monitoring and analysis operations.

- Supervising the COMSEC Material System (CMS) custodian in the execution of his duties and responsibilities for control and accountability over classified CMS material and equipment, including distribution and destruction of COMSEC material in accordance with current directives.
- Ordering COMSEC material and equipment for operations and exercises.
- Developing, in coordination with the unit security manager, emergency destruction plans for COMSEC materials and equipment.

b. G-2/S-2

- Advising and assisting the communications information systems officer on electronic protection techniques based on analysis of enemy SIGINT and EW capabilities and other threats to unit CIS and operations.

c. G-3/S-3

- Integrating communications information systems protection, including COMSEC and electronic protection, into the concept of operation in accordance with the commander's guidance.
- Planning and supervising the physical protection of essential communications nodes.
- Planning and supervising the overall EW effort in coordination with the G-2/S-2 and the G-6/S-6.

d. MEF COMSEC Management Office

- Providing and sourcing MEF units with mission essential contingency COMSEC material.
- Establishing CMS policy within the MEF.
- Deploying as a MEF COMSEC Management Office (MCMO) in support of the MEF or deploys and/or supports a Joint COMSEC Management Office for a Joint Headquarters.

e. Command Security Manager

- Serving as the commanding officer's advisor and direct representative in matters pertaining to the security of classified information and personnel security.

- Developing written command information and personnel security procedures, including an emergency plan which integrates emergency destruction bills where required.
- Ensuring that threats to security, compromises and other security violations are reported, recorded and, when necessary, investigated vigorously. Ensures incidents falling under the investigative jurisdiction of the NCIS are immediately referred to the nearest NCIS office.

For a complete list of all Security Manager duties/requirements refer to OPNAVINST 5510.1H.

7102. Cryptosecurity

Cryptosecurity is the COMSEC component that results from the provision of technically sound cryptosystems and their proper use. With the built-in encryption feature of SINCGARS and the widespread availability of encryption equipment for other SCRs and the SBB, it should be possible to cover all tactical communications. Accomplishing COMSEC requires detailed planning that is conducted as an integral part of the overall communications planning effort. The requirements for encryption must be determined and the appropriate equipment and material must be obtained to support those requirements. CJCSM 6231.05 provides detailed COMSEC information for TRI-TAC equipment and is a key reference in planning the SBB. Units must act immediately upon receipt of a COMSEC callout message to obtain the required cryptographic material to be employed in a particular exercise or operation to include, when designated, the intertheater COMSEC package. In the future, the joint key management system, which is under development, will enable the electronic distribution of keys throughout the JTF.

Modern cryptographic systems use random number generators to accomplish encryption. By initializing the random number generator with a seed number, a deterministic sequence of pseudorandom numbers is generated. Each time the same seed is used, the same sequence of numbers is generated. The pseudorandom numbers may then

be used, for example, to modify a bit stream to send over a communications network. If the receiver of the bit stream has access to the seed used by the sender, the modified bit stream can be decoded. The bit stream may consist of data, or it may be digitized voice. With this approach to encryption, it is not necessary for the equipment itself to be highly classified as was the case with World War II era encryption equipment. It is only losing the seed number, or key, that will compromise the encrypted information. Therefore, the management and control of keying material is of utmost concern. Commanders should limit the holdings of keying material to the minimum required for operations. This material must be transported, stored, safeguarded, destroyed, and accounted for in strict accordance with existing regulations.

7103. Transmission Security

Transmission security (TRANSEC) is that component of COMSEC that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. The Marine Corps' goal is to secure all tactical communications circuits and SCR nets. However, even encrypted communications may be targeted, exploited, and disrupted by an enemy's intelligence and EW organizations via traffic analysis, direction finding, and jamming. TRANSEC is an important component of the unit electronic protection effort.

a. SCR

Strict radio discipline and adherence to authorized procedures are key to ensuring TRANSEC over SCR networks. Operating SINCGARS radios in a frequency hopping mode provides maximum protection against enemy EW capabilities. Other TRANSEC measures include:

- Training operators thoroughly on proper communications procedures and equipment operation. (This includes all Marines that may operate SCR, not just CIS personnel.)
- Avoiding unauthorized transmission and testing and maximizing use of data networks to

minimize transmission time and opportunity for enemy direction finding.

- Using transmitter, antenna, and power combinations that produce minimum wave propagation and emission intensity consistent with reliable communications.
- Strictly adhering strictly to authorized frequencies.
- Using authentication systems to protect against imitative deception on nonsecure nets.
- Using changing call signs and frequencies on nonsecure nets.
- Promptly responding to and reporting enemy jamming. (Operators should continue to operate on assigned frequencies in a secure mode, unless otherwise directed by a competent authority, and should attempt to work through the interference.)
- Strictly adhering to all EMCON restrictions and observance of radio silence.
- Using communications means that do not radiate in the electromagnetic spectrum such as messengers, visual and sound signaling, and local wire loops.
- Using terrain masking to shield transmission systems from enemy EW systems.
- Remoting transmitters and avoiding the clustering of antennas.

b. Multichannel Radio and Wire

Information is often compromised by the assumption that wire is secure. While wire is inherently more secure than radio, the SBB normally uses MCR to move traffic beyond the local geographic area. Furthermore, when a wire infrastructure is used over an extended area, the line can be tapped. Sensitive traffic, voice or data, should be either sent over covered circuits or encrypted prior to transmission over nonsecure circuits. MCR operation in close proximity to the enemy is of concern because the high power of transmission equipment and continuous mode of operation are easily detectable and could potentially reveal the location of units and CPs. Use of terrain masking and, where possible, limiting forward and back lobe emission into enemy territory are measures

that can reduce the vulnerability of MCR to enemy EW.

In addition to encryption and measures to reduce the probability of interception, traffic flow security is required. Traffic flow security conceals the presence of messages on communications circuits. Traffic flow security is normally achieved on the SBB by using trunk encryption devices to generate a continuous stream of bits, making the circuit appear busy at all times.

7104. Emission Security

Emission security (TEMPEST) is the component of COMSEC that results from all measures taken to deny unauthorized persons information of value that might be derived from interception and analysis of compromising emanations from crypto equipment and telecommunications systems. The operation of communications and information systems may result in unintentional electromagnetic emissions. Although tactical equipment is designed to reduce the possibility of such emissions, COTS equipment is not. Unintentional emissions are extremely susceptible to interception and analysis and may disclose classified information. Commanders must follow applicable regulations providing guidance on control and suppression of such emissions.

7105. Physical Security

Physical security is the COMSEC component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access or observation by unauthorized persons. The access to classified cryptographic information must be tightly controlled. When a commander or designated representative has determined that an individual has a need to know and is eligible for access, then access to classified cryptographic information will be formally authorized. The authorization process must include an introduction to the unique nature of cryptographic information, its unusual sensitivity, the special security regulations governing its

handling and protection, and the penalties prescribed for its disclosure. In the event of a violation of physical security, a report is required. Reportable violations include:

- Loss of material.
- Unauthorized viewing.
- Capture of individuals having access to COMSEC information.

Currently fielded COMSEC equipment is unclassified for external viewing when appropriate covers are in place and no keying material is visible. Consequently, the exposure of such equipment to

casual viewing by uncleared personnel, whether by accident or as the result of operational necessity, does not constitute a reportable violation.

Personnel planning for and setting up the SBB must be aware of the requirement for red/black isolation. This refers to the separation of circuits, systems, equipment, and areas that handle classified plain text (red) information in electronic signal form from those that handle unclassified (black) information in electronic signal form. (Black signals include encrypted signals because these signals would not divulge national security information if recovered and analyzed.)

Section II

Computer Security

Command and control on the modern battlefield depends increasingly on information systems. The amount of data that is processed and the tempo of operations combine to make manual procedures inadequate except at the small unit level. Even at the small unit level, automated systems are proliferating, particularly in the fire support area. The increasing dependence on tactical information systems drives the requirement to protect these systems from disruption or exploitation by hostile forces. In much the same way that COMSEC provides the security for information transferred through communications systems, COMPUSEC provides the security for information that is collected, stored, processed, and displayed by computers and peripheral equipment at user locations.

7201. The Threat

With the openness of the Internet, intruders can inflict damage on information systems from virtually any location with little fear of detection. Today's information systems are connected into worldwide communications networks that are only as secure as the weakest link. The enemy can easily gain access to much of the same information infrastructure used by the MAGTF. Intruders do not require sophisticated technology. A non-technical means, such as a compromised password, can bypass LAN security features. Once access is gained, the attacker can employ malicious logic to inflict tremendous damage on our information systems. (Malicious logic is computer code designed to deny, destroy, modify, or impede system configurations, programs, data files, or routines. Types of malicious logic include viruses, Trojan horses, logic or time bombs, and worms.) The enemy will have several objectives in attacking MAGTF information systems.

a. Information Compromise

A major goal of threat attacks on MAGTF information systems is to gain access to classified or

sensitive information. Access to this information provides the enemy insight into MAGTF, joint, and national capabilities; force and resource locations; plans and intentions; readiness status; and knowledge of what is known about the enemy. This type of information, when discovered and used to advantage, has often been the deciding factor in the outcome of battle. In today's environment, this type of information is surprisingly easy to obtain. For example, careless e-mail exchanges with family and friends can reveal planned MAGTF movements and operations. E-mail is easily and readily collected by enemy agents.

b. Information Modification

Another objective of attacks on our information systems is information modification. Such information corruption can be used to create an electronic deception. Undetected, it can lead to incorrect assumptions and subsequent faulty decisions. In other instances, the attack may be designed to destroy information required to execute the MAGTF planning and decision cycles. In either case, detection of the attack can severely reduce confidence in the MAGTF's information systems. The MAGTF's ability to observe, orient, decide, and act more quickly than the enemy depends greatly on the information provided by the information systems used. Reduced confidence, induced time delays, and undetected, faulty information can all severely degrade the commander's ability to make sound and timely decisions.

c. Denial of Service

Still another objective of enemy attacks on our information systems is either total or partial restriction of our ability to process, retrieve, and disseminate information. Data corruption results in lost confidence and service self-denial. Successful enemy attacks on stored data, applications, or operating systems may render information systems unusable. Damage or physical destruction to equipment, facilities, and per-

sonnel will be a high priority for the enemy because our communications information systems capabilities are viewed as critical vulnerabilities and key targets. Such attacks may range from terrorist truck bombings to more technologically advanced enemies using directed energy weapons. The environment is also a potential disruptive force. Information systems, particularly COTS systems, are very susceptible to power surges; temperature extremes; and dusty, dirty, and sandy conditions encountered in the austere littoral areas in which the MAGTF operates.

7202. Protection

Protection of MAGTF information systems is essential. COMPUSEC is the means of providing that protection. This includes knowledge of the threat and employment of operating procedures, equipment, and personnel training to counter that threat. COMPUSEC also includes putting into place measures to detect intrusion early and planning for immediate action to counter attacks, and, if necessary restore lost data and service.

a. Responsibilities

COMPUSEC is a command responsibility and must be understood and practiced by all MAGTF information systems users. However, overall network and information systems security responsibility belongs to the CISO. This includes establishing policy and procedures for LAN, WAN, and information systems management. Procedures are required to manage user identification and passwords assignment, to provide authentication, and to maintain visibility and control of the operation and use of network services. The CISO coordinates network management functions, including security, with the individual LAN managers and information systems coordinators. Training and education in threat capabilities and COMPUSEC procedures are CISO's responsibility, supported by the unit security manager, G-2/S-2, G-3/S-3, and in coordination with all LAN managers and functional information systems coordinators.

b. Management

The CISO provides overall COMPUSEC management through policies, directives, plans, and training. The CISO guides LAN managers, information systems coordinators, and information systems users in implementing procedures necessary to maintain reliable and secure information systems. Much of the security for information systems is provided at the individual workstation through operating systems and application-specific access mechanisms. However, for networked applications and services, a well-devised network security plan is necessary to manage the various accesses and privileges that control read and write access to files and data. Monitoring the network is required to document activity and detect intruders. COMPUSEC procedures must be integrated with and complement the overall communications information systems plan to ensure responsive service to authorized users while protecting against unauthorized access.

c. Implementation

DOD Directive 5200.28 establishes mandatory, minimum standards for automated information systems. It promotes using computer-based security features that emphasize the personal responsibility of system users. Current procedures rely on standalone workstations and system high networks, which require dedicated routers and switches, making system security management difficult. There are many ongoing programs to provide improved security services for individual workstations, LANs, and the overall DII. Multi-level Information Systems Security Initiative products and services are being fielded incrementally as technology matures. They include—

(1) Cryptographic Cards. PC-configured cryptographic cards are gradually being introduced to provide different levels of personal security protection, including confidentiality, data integrity, identification/authentication, and nonrepudiation.

(2) Firewalls. Firewalls protect MAGTF networks from outside networks such as the Internet. Firewalls with Fortezza identification and authentication allow Fortezza card-holders controlled access to the NIPRNET from outside networks. This

capability prevents unauthorized access to the sensitive but unclassified information on the NIPR-NET while providing convenient access for authorized users.

(3) High Assurance Guards. High assurance guards, such as the secure network server with standard mail guard, are used to protect against unauthorized release of classified information from a classified facility while allowing the release of unclassified information. High assurance means that the guard has been verified by the National Security Agency to be highly resistant to penetration based on the application of rigorous security software engineering methods, extensive penetration testing, and security analysis during its development, production, and fielding. The guard is required for information processing and exchange between facilities or systems operating at different levels. The guard also ensures that external requests for access to the “guarded” higher security level locations are approved before allowing that access.

(4) In-Line Network Encryptor. In-line network encryptors provide data confidentiality and integrity across LANs and WANs. They employ encryption and access control through cryptographic key management. Some in-line network encryptors can also provide traffic flow security services. In-line network encryptors operate with IP routers, packet switches, synchronous optical networks, and asynchronous transfer mode networks. Some of the in-line network encryptors offer combinations of these capabilities to allow for the future growth of networks based on synchronous optical network and asynchronous transfer mode technologies. A key feature of in-line network encryptors is that they encrypt only the data, not the address

information. This allows the transmission of classified data on unclassified networks or SCI data on secret networks. In-line network encryptors, through software configuration and appropriate keying material, are used to link multiple sites.

(5) Security Management Services. Security management services include security measures such as cryptographic keying, access control, authentication, and the use of passwords. These services are needed to implement effective information systems security programs within the MAGTF. Key security management services include—

- Local authority workstations that reside on the LAN and provide security capabilities such as digital signatures, cryptographic keys, and access control permissions.
- Rekey managers that work in conjunction with electronic key management systems to provide cryptographic rekey support for Multilevel Information Systems Security Initiative products.
- Audit managers that provide support for the collection and analysis of security-relevant events that can be audited and are associated with Multilevel Information Systems Security Initiative products. Repeated failed user login is an example of a security-relevant event that can be audited.
- Directories that provide a repository for public security information essential for effective global message addressing. The public part of a user’s digital signature is an example of this type of public security information.
- Mail list agents that are used by messaging systems to add security for messages that are sent to many recipients.

Section III

Incident Response

Effective response to attacks on MAGTF information systems requires that all users and support personnel be aware of attack indicators and the procedures to be followed in the event of an attack. The Marine Corps Command Center (MCCC) and the Network Operations Center (NOC) will exchange information in the event of an INFOSEC incident. The MCCC will act as the communications link between the NOC and Headquarters Marine Corps throughout the incident. The NOC has the overall responsibility of managing any computer intrusion incidents in the Marine Corps.

7301. The Fleet Information Warfare Center

The Fleet Information Warfare Center is the Navy's principal agent for development of information warfare and command and control warfare tactics, procedures, and training. The center deploys personnel trained in command and control protection and is equipped with appropriate information systems security equipment to support battle group and JTF operations. It is responsible for providing computer incident response teams and is the single point of contact for monitoring the security of information systems. All computer incidents (break-in attempts and malicious logic) are reported to the center. The center publishes advisories containing the latest information on system vulnerabilities and effective countermeasures. These advisories are received from the center's computer incident response team by the Marine Corps Network Operations Center and disseminated to all Marine Corps commands.

7302. Naval INFOSEC Help Desk

The information systems security help desk at Naval In-Service Engineering Activity on the East Coast provides expert assistance with all informa-

tion systems security and computer security problems. This help desk receives calls 24 hours daily and is manned a minimum of 8 hours per day, Monday through Friday. Emergency calls are received via cellular phone when the help desk is not manned. Services include—

- Security policy interpretation.
- Installation, configuration, support, and training for implementation of network security products:
 - Internet firewalls.
 - Standard mail guard.
 - Secure network server.
 - Fortezza cards.
 - Packet filters and routers.
 - UNIX host security.
- Additional guidance is provided on—
 - The Multilevel Information Systems Security Initiative.
 - Protected distribution systems.
 - Secure systems and Tempest certifications.
 - Cryptographic/COMSEC equipment.
 - Secure voice systems.
 - The Navy Key Management System.
 - Secure telemetry and communications.
 - Computer and network security tools.
 - Risk assessment and vulnerability surveys.
 - Destruction, purging, or recovery of sensitive data.
 - Computer systems accreditation and certification.
 - Controlled access.
 - Distribution of naval computer security publications.
 - Training courses.
 - Other naval INFOSEC resources.

7303. The Air Force Information Warfare Center

The Air Force Information Warfare Center develops, maintains, and deploys command and control warfare capabilities in support of operations, campaign planning, acquisition, and testing. The center acts as the single focal point for command and control warfare services and provides technical expertise for computer security and COMSEC. The Air Force computer emergency response team is part of the center and is responsible for reporting and handling computer security incidents and vulnerabilities. The center publishes advisories containing the latest information on system

vulnerabilities and effective countermeasures. These advisories are received by the Marine Corps Network Operations Center and disseminated to all Marine Corps commands.

7304. Points of Contact

Appendix N provides points of contact, including telephone numbers, WWW uniform resource locators (URLs), and e-mail addresses, for INFOS-EC and other key organizations. Appendix P includes a list of reference documents. This information should be verified and incorporated into command and control plans and SOPs.

Chapter 8

Future Directions

The Marine Corps implementation of command and control is based on a maneuver warfare philosophy. Effective support of maneuver warfare demands a flexible command and control system that can support rapid decisionmaking and execution to create and maintain a high tempo of operations. CIS and equipment are the means through which effective command and control support is provided. These systems must be as robust, flexible, and expeditionary as the MAGTF they support. They are employed across the full spectrum of operations, from humanitarian assistance operations to general war. They support the MAGTF whether forward deployed or in garrison.

Most importantly, MAGTF CIS must be equally capable of supporting all expeditionary operations conducted by the Marine Corps—operational maneuver from the sea (OMFTS), sustained operations ashore, and military operations other than war (MOOTW). This chapter focuses on OMFTS, the concept by which naval forces will project power ashore in the 21st century. As the command and control doctrine and organizations evolve to meet the requirements of OMFTS, MAGTF CIS and equipment must evolve as well. This chapter provides a framework for understanding the unique considerations in the employment of CIS to support OMFTS.

8001. Operational Maneuver from the Sea

The underlying operational concept for all MAGTF operations is OMFTS. This concept is the application of the principles of maneuver warfare to naval forces at the operational level. While not every MAGTF operation is an OMFTS, the maneuver warfare principles associated with it provide the basis for all Marine Corps operations.

In OMFTS, the MAGTF operates as part of a naval expeditionary force in the conduct of a joint campaign. The primary focus of OMFTS is to allow a sea-based MAGTF to decisively engage enemy forces and accomplish naval and joint objectives. New technologies and capabilities in amphibious operations will allow the MAGTF to engage the enemy from positions of advantage and to penetrate to the heart of an enemy system, destroying his ability and will to resist effectively.

OMFTS may allow the MAGTF to act as an enabling force, allowing the introduction of larger land-based forces to commence sustained operations ashore; as a decisive force, where the MAGTF operates to achieve the decisive campaign objectives of a joint force commander; or as an exploitation force that takes advantage of opportunities created by other elements of the joint force. The transition to sustained operations ashore (SOA) or other expeditionary operations (OEO), and the decision to base all or some of the MAGTF ashore for long periods will depend on the situation and assigned missions. OMFTS is based on two key implementing concepts—ship-to-objective maneuver (STOM) and seabasing.

a. Ship-to-Objective Maneuver

The implementing concept of STOM combines the ship-to-shore movement with subsequent operations ashore into a single, decisive maneuver directly from the ship. STOM generates operating tempo by avoiding a pause to build up combat power ashore. Full exploitation of this concept hinges on fielding the advanced amphibious assault vehicle (AAAV) and the MV-22 to transport the surface assault and the vertical assault, respectively. However, through skillful use of available platforms, STOM is possible today, although on a somewhat restricted scale. Figure 8-1 (on page 8-2) depicts the STOM concept.

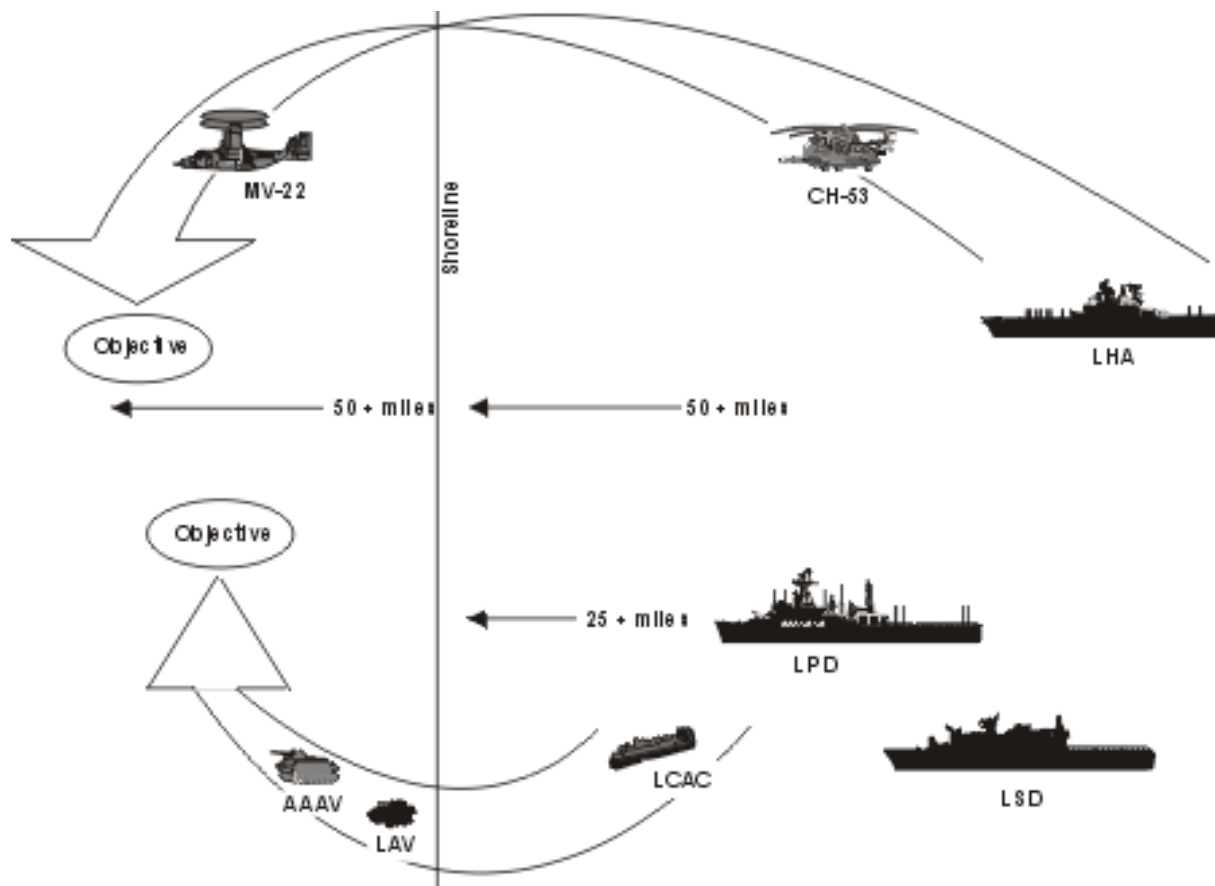


Figure 8-1. The STOM Concept.

b. Seabasing

Seabasing is another important implementing concept for executing OMFTS. Seabasing envisions bringing ashore only those MAGTF elements that must be ashore to accomplish their mission. Most fire support, command and control, and logistic functions remain at sea throughout the operation. Most aviation support remains sea-based. While some or all GCE C2 transitions ashore, the overall command and control of the MAGTF, centralized in the MAGTF CE, normally stays afloat. Seabasing offers tremendous operational freedom of action to the MAGTF. Retaining command and control, aviation, fires, and logistics afloat reduces the need to establish and then protect shore-based facilities while simultaneously enhancing the MAGTF's force protection posture. This translates into increased operating tempo and reduced requirements for rear area security. The reduced infrastructure ashore also facilitates the rapid reembarkation and redeployment of the landing force.

8002. CIS Requirements

OMFTS provides a means of projecting naval expeditionary power directly against an exposed enemy center of gravity (COG) or critical vulnerability. However, the execution of OMFTS poses a number of C2 challenges, particularly with respect to CIS support. Perhaps the most obvious challenge is how to provide secure, reliable, high-capacity communications links over extended distances, perhaps as much as 200 miles, from the ships of the ATF to rapidly maneuvering surface and vertical assault elements ashore. For longer distances, innovative solutions and new uses for existing equipment must be pursued. Satellite communications (SATCOM) offers the best near term solution. Airborne/ground-based high capability, multichannel relay sites; long range, high capacity single channel systems; and secure global cellular and phone networks are just some of the intriguing possibilities to provide ship-to-objective communications.

In the near-term, several interim fixes are being pursued, including the possible employment of the MRC-142 with appropriately modified antennas to enable shipboard operation providing connectivity at ranges of up to 40 miles. For longer distances, SATCOM appears to be the only currently available option. Although the numbers of SATCOM terminals currently available are relatively limited, this situation is improving with the fielding of the AN/PSC 5. However, obtaining the SATCOM access required to provide the communications connectivity needed for command and control of a MEF is problematic because of competition with other elements of the ATF, the naval expeditionary force, and the JTF. Before and during the early phases of the ship-to-shore movement, ultrahigh frequency (UHF) tactical satellites (TACSATs) with high frequency (HF) single channel radios (SCR) as backup is the predominant means of long-haul communications.

Once established ashore, MAGTF forward elements may use ground mobile forces (GMF) TACSAT. As previously discussed, employment of high-capacity, multichannel transmission systems and establishment of the switched backbone come at some expense in terms of maneuverability. Tradeoffs will demand careful analysis. Future systems should seek to overcome these limitations.

Another key ingredient for successful OMFTS is the provision of real-time COP throughout the ATF and the landing force. OMFTS depends on free maneuver of both the surface assault and the vertical assault elements to exploit the developing situation and to avoid obstacles and strongpoints. The only way that we can maneuver freely while simultaneously providing responsive supporting fires is through continuous, real-time knowledge of friendly and enemy locations. Presently, this position location information (PLI) is available through the PLRS system installed aboard the LHD class of amphibious ships and can be disseminated throughout the ATF by JMCIS. Shipboard coverage of landing force maneuver elements must be maintained until the landing force brings a master station ashore. Depending on the distances involved, relay units, either sur-

face or airborne, may be required for effective PLRS operation. Future systems will exploit PLRS, GPS and other navigation systems, linked to communication and information systems, to provide an accurate, real time COP throughout the MAGTF and Navy force.

To conduct OMFTS, the MAGTF must have the ability to employ its information systems effectively while at sea. This is an area in which significant improvements are rapidly occurring. Both tactical combat operations (TCO) and intelligence analysis system (IAS) are routinely deployed aboard amphibious ships, and connectivity is being provided to the JMCIS LAN. However, presently these installations are occurring on an ad hoc basis, and the installation varies from ship to ship even within the same class. It is therefore critical that the command and control officer begin planning early to ensure not only adequate numbers of workstations, but also, just as importantly, adequate LAN connectivity. Workstations dedicated to MAGTF LAN connectivity are required in all landing force command and control and administrative work spaces in all ships of the amphibious ready group, not just in the LFOC aboard the flagship. Future seabased MAGTF facilities will require CIS connectivity that is as effective throughout the battle space as that for shore based facilities. In other words, whether seabased or shore-based, CIS capabilities and availability should be transparent to users in future command naval control and administrative facilities.

Full implementation of OMFTS will place stringent demands on the command and control capabilities of the MAGTF. The MAGTF will exercise command and control both ashore and afloat over greatly extended distances. Furthermore, the MAGTF will depend on increasing amounts of information to plan operations, deploy and sustain its forces, and execute its missions. Effective information management will be critical for focused, efficient command and control. Information systems must provide a common picture of the battlefield and shared situational awareness throughout the battlespace. Communications systems must provide a robust voice and

data communications capability throughout the battlespace and connectivity to information resources throughout the world.

The CIS discussed in chapters 3, 4, and 5 will provide many of these capabilities in the near future. This includes the migration of tactical information systems to the GCCS and the fielding of internet protocol (IP) router and IDNX-based gateways and servers. Continual improvements in the packaging of tactical information systems will result in smaller, more maneuverable operations centers and CPs. Another significant development is the JTF enabler, which will allow a MEU(SOC) to provide initial communications

and information systems support to a follow-on forces commander.

As a final note, MAGTF operational concepts are undergoing rapid and dramatic change, not unlike the field of information technology. MAGTF communications and information systems personnel must adapt the command and control system to support these evolving concepts. This will be done through exploitation of information technology and the continued refinement of proven command and control doctrine. The ultimate goal is to enhance the commander's command and control capabilities—providing the necessary information at the right place and time for effective planning, decisionmaking, and execution.

Appendix A

Defense Information Infrastructure Common Operating Environment Compliance

The concept of a common operating environment (COE) is the most significant part of the Global Command and Control System (GCCS) development effort. The DII COE encompasses the architecture, standards, and reusable software modules that provide a cohesive framework for systems development. Even more importantly, the DII COE guarantees the interoperability of all systems that achieve full COE compliance. This appendix addresses what is meant by COE compliance. As with any standard, compliance is required to ensure interoperability. More detailed information on the DII COE and COE compliance may be found on the Defense Information Systems Agency (DISA) COE configuration management web site—http://spider.osfl.disa.mil/cm/1097_cm_page.html. The information in this appendix is extracted from DII COE Version 3.0 of 5 February 1997.

Compliance Categories

The DII COE defines four areas of compliance called compliance categories. Within a specific category, a segment is assigned a numerical value, called the compliance level, which is a measure of the degree to which a segment is compliant within the category. This approach facilitates the development of migration strategies for legacy systems as well as the evaluation of COE compliance by both legacy systems and new developments.

Category 1, Runtime Environment

Category 1 measures how well the proposed software fits within the COE executing environment and the degree to which the software reuses COE components. It is an assessment of whether the

software will run when loaded on a COE platform and whether it will interfere with other segments.

Category 2, Style Guide

Category 2 measures how well the proposed software operates from a look and feel perspective. It is an assessment of how consistent the overall system will appear to the *end user*. It is important that the resulting COE-based system appear seamless and consistent to minimize training and maintenance costs.

Category 3, Architectural Compatibility

Category 3 measures how well the proposed software fits within the COE architecture (client/server architecture, distributed computing environment (DCE) infrastructure, CDE desktop, etc.). It is an assessment of the software's potential longevity as the COE evolves. It does not imply that all software must be client/server and remote procedure call (RPC)-based. It simply means that a reasonable design choice has been made given that the COE is client/server based and is built on top of a DCE infrastructure.

Category 4, Software Quality

Category 4 measures traditional software metrics (lines of code, McCabe complexity metric, etc.). It is an assessment of program risk and software maturity.

Category 1 Levels

Version 3.0 of the COE defines compliance levels for category 1 only. The COE defines eight progressively deeper levels of integration for this category. Levels 1 through 3 are considered to be

interfacing with the COE and not integrated with the COE. Integration begins at level 4.

Bootstrap compliance (level 4) is required before a segment may be submitted to DISA for evaluation as a prototype. Such segments will not be fielded or accepted into the online library. At DISA's discretion, segments that meet the criteria for minimal COE compliance (level 5) may be accepted into the online library and installed at selected sites as prototypes for user evaluation and feedback. However, such segments will not be accepted as fieldable products. Acceptance as an official DISA fieldable product requires demonstration of interoperable compliance (level 7) and a migration strategy to full COE compliance (level 8), unless the proposed segment is an interim product that is targeted to be phased out in the near term.

As previously noted, the compliance categories and levels are designed to support the migration of legacy systems into the COE. The first step of category 1, covered by levels 1 through 4, is to ensure that systems do not destructively interfere with each other when located at the same operational site. Level 5 is sometimes called a federation of systems in that while systems are still maintained as stovepipes, they can safely share common hardware platform resources. Levels 6 through 8 complete the migration by reducing functional duplication, promoting true data sharing, and making the system appear to the user as if it were developed as a single system. The last three levels represent varying degrees of integration from marginally acceptable (level 6) to a truly integrated system (level 8).

Level 1, Standards Compliance

Level 1 is a superficial level in which the proposed capabilities share only a common set of COTS standards. Sharing of data is undisciplined, and minimal software reuse exists beyond the COTS. Level 1 may allow simultaneous execution of the two systems.

Level 2, Network Compliance

Two capabilities coexist on the same LAN but on different central processing units (CPUs). Limited data sharing is possible. If common user interface standards are used, applications on the LAN may have a common appearance to the user.

Level 3, Workstation Compliance

Environmental conflicts have been resolved so that two applications may reside on the same LAN, share data, and coexist on the same workstation as COE based software. The kernel COE, or its equivalent, must reside on the workstation. Segmenting may not have been performed, but some COE components may be reused. Applications do not use the COE services and are not necessarily inter operable.

Level 4, Bootstrap Compliance

At level 4, all applications are in segment format and share the bootstrap COE. Segment formatting allows automatic checking for certain types of application conflicts. Use of COE services is not achieved and users may require separate login accounts to switch between applications.

Level 5, Minimal COE Compliance

At this level, all segments share the same kernel COE, and functionality is available via the executive manager. Boot, background, and local processes are specified through the appropriate segment descriptor files. Segments are registered and available through the online library. Applications appear integrated to the user, but there may be duplication of functionality and inter operability is not guaranteed. Segments may be successfully installed and removed through the COE installation tools.

Level 6, Intermediate COE Compliance

Segments use existing account groups and reuse one or more COE component segments. Minor documented differences may exist between the style guide and the segment's graphical user interface (GUI) implementation.

Level 7, Interoperable Compliance

Segments reuse COE component segments to ensure inter operability. These include COE provided communications interfaces, message parsers, database tables, track data elements, and logistic services. All access is through published application program interfaces with documented use of few, if any, private application program interfaces. Segments do not duplicate any functionality contained in COE component segments.

Level 8, Full COE Compliance

Proposed new functionality is completely integrated into the system (e.g., makes maximum possible use of COE services) and is available via the executive manager. The segment is fully compliant with the style guide and uses only published public application program interfaces. The segment does not duplicate any functionality contained elsewhere in the system whether as part of the COE or as part of another mission application segment.

Appendix B

Common Hardware and Standard Commercial Software Applications

MAGTF units employ a wide and varied array of computers and peripheral equipment. Although some of this computer hardware represents the latest technology in the commercial market, in many instances, constrained budgets force units to continue to use some outdated, yet still functioning, equipment. This situation is a fact of life in the FMF and is manageable through proper training and effective maintenance practices. However, such equipment will ultimately become more expensive to maintain than to replace.

Standard commercial software is identified by Requirements Division, Marine Corps Combat Development Command. These standards are promulgated to improve interoperability and reduce training requirements.

Computers are used throughout the MAGTF both as integral components of tactical information systems and for administrative and logistic support functions. Several fielded tactical information systems including TAOM and PLRS use embedded Navy standard AYK and UYK computers, which will not be addressed here. As new MAGTF C4I systems are developed and fielded systems mi-

grate to the DII COE, they are hosted on a standard suite of computers—the Marine common hardware suite (MCHS).

The Marine Common Hardware Suite

The Common Computer Resources (CCR) Program Office, Marine Corps Systems Command, continuously evaluates computers and peripheral equipment for inclusion in the MCHS and identifies DOD contract vehicles (currently Navy- and Army-common hardware programs) to use for procurement by the MCHS. This office maintains a *Computer Buyer's Guide* that is updated on a quarterly basis and posted on the Marine Corps Systems Command web site (www.marcorsyscom.usmc.mil). Procurement of common computer resources through the MCHS program will help ensure commonality, interoperability, supportability, and redundancy between the computers and peripherals that support the many functional users. Figure B-1 depicts the categories of MCHS equipment currently available through the CCR contracts.

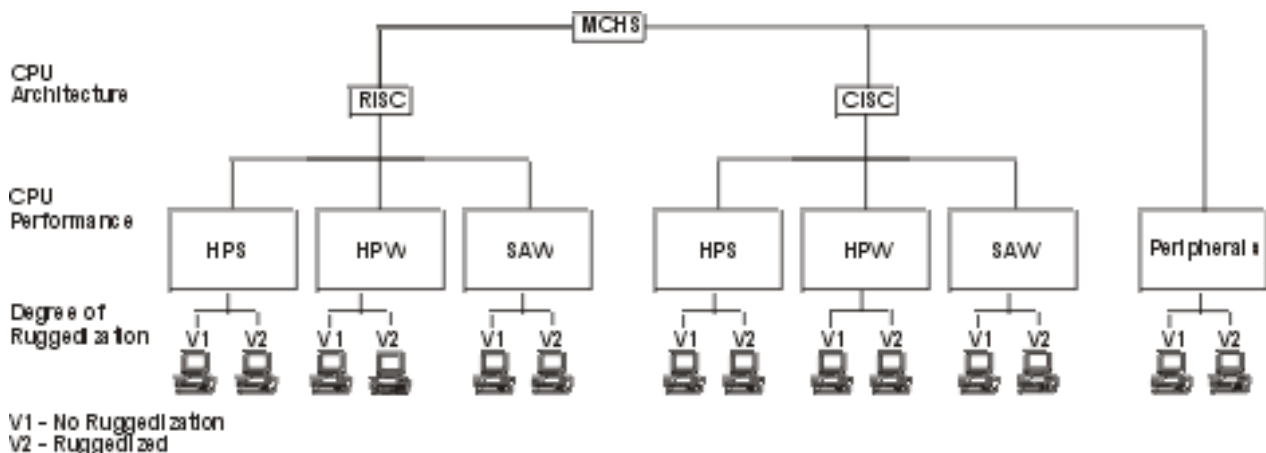


Figure B-1. The MCHS.

MCHS High-Performance Server

The high-performance server (HPS) is intended to function as a network server, database server, and communications server, or as a central facility processor with rapid processing and display capabilities. It is intended for medium-to-large-sized workgroups that use processor-intensive applications. HPS computers are available in both UNIX-compatible, reduced instruction set computing (RISC) and PC-compatible, complex instruction set computing (CISC) architectures. The HPS RISC and CISC computers are also available in both nonrugged (V1) and rugged (V2) variants. Variant 2 is configured to fit into a 19-inch rack. Peripherals available for the HPS include CD-ROM, erasable optical disks, digital audio tape (DAT) drives, high-capacity internal storage disks, an expansion chassis, enhanced graphics capability, and various video monitors.

MCHS High-Performance Workstation/ Application Server

The high-performance workstation (HPW) has the capability to function as a server for smaller workgroups and as a network or standalone workstation. The HPW is available in the same computing architectures and variants as the HPS. Variant 1 is available in desktop/deskside and portable configurations. Variant 2 is available in a portable configuration.

MCHS Standard Application Workstation

The MCHS standard application workstation (SAW) provides network and standalone, high- and low-end, desktop or laptop computers for use at all echelons of the MAGTF. The SAW computers are available in the same computing architectures and variants as the HPS and HPW computers. Peripherals available for the SAW include CD-ROM, a tape drive, a high-capacity removable disk drive, external video monitors, Ethernet LAN interface cards, a ruggedized magneto-optical drive, and others.

Peripherals

Peripheral equipment includes items purchased separately, such as printers, facsimile modems

and machines, data storage devices, UPSs, and various types of displays. Some of these devices are purchased as standard equipment through the supply system, and others are obtained as COTS products. Additionally, many peripheral components are provided as part of the MCHS equipment fielded for various command posts and centers. Proper operation of this equipment involves using quality cables and ensuring that proper connections are maintained to computing and LAN equipment. Most peripherals also require software drivers that must be installed with the appropriate user preferences and settings. Table B-1 lists some typical peripheral equipment used with MAGTF information systems.

Data Storage

The MCHS provides a separate four-bay SCSI peripheral device enclosure, commonly referred to as the TAC-4 Data Silo. This enclosure accommodates two 2.5 GB (4 GB optional) removable disks, a CD-ROM drive, and a 4-mm DAT drive. The TAC-4 Data Silo is connected to the workstation via an SCSI port. This item is a part of the MCHS suite of equipment.

I/O

The SCSI provides a commercial standard computer interface for peripheral devices. The SCSI terminal server is a separate SCSI peripheral device that provides eight RS-232 serial ports and one parallel port as a means of connectivity to other devices. This item is a part of the MCHS suite of equipment.

Printer

The MAGTF MCHS printers include both PaintJet and DeskJet printers. These printers are available in both color and black and white for hard-copy text and graphics output.

Plotter

The recommended MCHS plotter is a DesignJet model.

Scanner

The recommended MCHS scanner is a ScanJet model.

Display

The large group display is composed of a flat-panel video display that rests on top of a high-intensity overhead projector to project the workstation screen displays. This item is a part of the MCHS suite of equipment.

Power Supply/Protection

UPSs protect computers from the power surges of field-generated power. The UPS also provides a backup power source.

End-User Computing Equipment

The End-User Computing Equipment (EUCE) Program fields microcomputer systems throughout the FMF for general-purpose administrative information processing and for information system workstations. The EUCE, AN/UYK-83, and the downsized version, DEUCE, AN/UYK-85, are ruggedized, Tempest-certified 286, 386, and 486 IBM-compatible computers. These computers are being replaced by more capable computers purchased through the MCHS program.

Table B-1. MCHS Peripheral Equipment.

Category	Peripheral Equipment
Storage	Z-Micro single, dual plus, three-bay, four-bay, and seven-across expansion chassis with removable hard drives and media canisters
Input/Output (I/O)	SCSI Terminal Server
Printer	Hewlett-Packard DeskJet and LaserJet Models
Plotter	Hewlett-Packard DesignJet Models
Scanner	Hewlett-Packard ScanJet Models
Display	Large Group Display Flat-Panel Video Display
Power Supply	UPS Rugged COTS

(reverse blank)

Appendix C

Ship Visit Checklist

Action Items

Ship visits are conducted by the CIS officer before embarkation. CIS representatives embarked aboard the same ship should coordinate a joint meeting. CIS requirements have to be completely coordinated with the ship's information officer so that an exchange of information, decisions, plans, orders, and instructions may be properly executed. Every attempt should be made to get a written agreement by all concerned. Key considerations during ship visits follow.

In Preparation

- Determine communications center requirements (number of augmentees).
- Determine circuit requirements.
- Determine TECHCON capabilities.
- Identify classified material and CMS storage needs.
- Identify HAZMAT storage needs.

During Ship Visit

- Determine space available for landing force:
 - Communications control
 - Message reproduction and distribution
 - CIS officer and staff office
 - Cryptographic material and equipment storage
 - Battery storage
 - CIS equipment repair benches
 - Radio central
 - Troop training spaces.
- Locate joint spaces (joint intelligence center, SACC, etc.).
- Provide prioritized list of landing force circuit requirements (by type operation).

- Discuss ship's ability to meet landing force needs.
- Discuss equipment type, operational condition, and interoperability.
- Identify shortfalls.
- Discuss deck mounting policy (i.e., location, type of equipment, security, and safeguarding of ship's watertight integrity).
- Provide guard list and summary of anticipated arrivals and departures.
- Discuss communications center and other shipboard personnel augmentation requirements.
- Discuss message quantities and distribution procedures for landing force message traffic.
- Obtain copy of *Ship's Loading and Characteristics Pamphlet* (SLCP).
- Review SLCP for accuracy.
- Review Marine tactical CIS systems and/or communications detachment SOP(s).
- Identify shipboard CIS available for landing force use. (See list at end of this checklist.)
- Coordinate EMCON notification-of-change procedures.
- Discuss joint circuits and facilities to be used during each phase of the operation.
- Resolve location, quantity, and restoration priorities of landing force circuits. Get a copy of the phone directory for the ship's spaces to prepare a phone directory for all landing force spaces (including berthing and state rooms) and other critical spaces aboard the ship.

Also Discuss:

- Antenna locations
- Frequency separation requirements
- Shipboard interference problems
- Joint intelligence center communications

- How to handle high-precedence and special-category landing force message traffic
- SCI communications
- Access lists
- Remote locations
- Use of signal communications during EMCON
- Supplies and communications center operating stocks to be provided by landing force
- Fleet secure voice communications (FLTSE-VOCOM) channelization
- Competing requirements/potential problem areas
- Lost communications procedures
- Window versus carrier frequencies
- Telephone locations
- Multichannel channelization
- Clearance and message-release needs
- Use of brevity codes, authentication, and so on
- Types of information systems available
- Availability of Navy and Marine Corps CIS operators, maintainers, and supply support personnel
- Operational checkout of shipboard equipment designated for landing force use
- LAN connectivity to “green spaces”
- FCC-100 (SHF) channelization (satellite access request coordination)
- DSN trunks
- JDISS
- GCCS
- TCO, IAS, AFATDS, Logistic AIS (LOGAIS), etc.
- IP addresses
- Use of copiers/printers/scanners
- INMARSAT
- NIPRNET
- SIPRNET
- JWICS
- Unique systems (PLRS/KSQ-1, situational awareness beacon with reply (SABER), enhanced PLRS)

- Plain old telephone system (POTS)
- KY-68 (connection to Pentagon red switch)
- EHF capabilities

Shipboard CIS

The following CIS represent the types of systems found aboard amphibious ships in the fleet. This list is not all inclusive; it is meant to stimulate thought and lead to a constructive dialog among embarking Marine and ship's company CIS personnel. Systems will vary widely among ships of the same type and among different types of ships. This is because all ships are rotated periodically through service life extension program overhauls where they receive new systems and system upgrades that are planned through the combat development process.

C2

- JMCIS Unified Build 1.X, 2.X, 3.X, etc.
- CTAPS host/remote
- CTAPS 5.2 (TAC *n*)
- Joint Maritime Tactical Communications Switching System (JMTCSS) (formerly TRI-TAC and smart multiplexing unit (SMU))
- Integrated Video System (23TV) closed-circuit television video switch
- Radiant Mercury A rules-driven multilevel security automatic sanitizer
- AN/USQ-119D, NTCS-A IV
- GCCS phase 2 or 3
- 9TV (SXQ-8)

Satellite Communications

- INMARSAT A/B
- W-band commercial SATCOM
- EHF SATCOM USC-38
- Navy EHF communications controller (NECC)
- EHF medium data rate (MDR) MILSTAR
- High-speed fleet broadcast
- WSC-3 UHF SATCOM/line of sight

- WSC-6 SHF SATCOM/7' antenna
- Global Broadcast Service (GBS)/Joint Broadcast Service (JBS)
- UHF DAMA
- 5 kHz DAMA AN/USC-54

Logistics

- Naval Tactical Command Support System (NTCSS) includes the following:
 - Shipboard Nontactical Automated Data Processing (ADP) Program (SNAP): includes automated supply, financial, organizational maintenance management, administration, and medical functions
 - Naval Aviation Logistics Command Management Information System (NALCOMIS): includes intermediate and organizational-level maintenance management
- Maintenance Resource Management System (MRMS): automates shipboard intermediate maintenance management.

Communications

- Joint Maritime Communications Strategy (JMCOMS) includes—
 - Automated Digital Network System (ADNS): network management, switching, routing, and control
 - Digital Modular Radio (DMR) System: multifunction radio (2 kHz - 2 GHz)
 - Integrated Terminal Program (ITP): military and commercial radio at frequencies above 2 GHz.
- Link 4A air intercept control and fighter-to-fighter data link
- Link 11 AN/USQ-125 common shipboard data terminal set (CSDTS)
- Link 16 (JTIDS)/command and control processor rehost
- Officer in Tactical Command Information Exchange System (OTCIXS)
- TACINTEL (UHF Fleet SATCOM Subsystem)/TACINTEL II Plus

- Tactical Data Information Exchange System-Subsystem A (TADIXS-A)
- TADIXS-B tactical receive equipment
- JTT/commander's tactical terminal (CTT)
- Battle Group Information Exchange System (BGIXS)

Tactical Communications

- Mission Display System
- Battlegroup cellular telephone system
- Maritime Cellular Information Exchange System (MCIXS)
- High-frequency radio group (HFRG)
- R-2368A HF/low frequency-medium frequency receiver
- SINCGARS (3 channel)
- UHF Digital Wideband Transmission System (DWTS)
- UHF antijam HAVE QUICK
- Video Information Exchange System (VIXS)

Intelligence-IW Sensors

- JWICS
- JDISS
- Battle Group Passive Horizon Extension System (BGPHEs)
- Common high-bandwidth data link (CHBDL)
- Outboard/combat direction finding
- Ship's signals exploitation equipment
- JSIPS-Navy (JSIPS-N)
- DSSCS
- TACINTEL
- Tactical Remote Sensor System (TRSS)

Message Processing

- NAVMACS I/II
- AN/SSQ-33A Shipboard Automated Communications Control System
- UGC-143A(V) Navy standard terminal (NST)
- Navy orderwire

Miscellaneous CIS Equipment

- Red analog switch
- Black analog switch
- Battlegroup HF e-mail
- Information transfer for the 21st century (IT-21)
- IT-21 DNS-GENSER
- IT-21 DNS-SCI
- Red/black baseband switch
- SSQ-88C Quality Monitoring System
- Electronic Key Management System Phase 2
- Navy Key Management System local management device

Appendix D

MAGTF Radio Nets

This appendix provides the basic description and participants for each radio net. It is a planning guide for radio nets that may be established to satisfy MAGTF CIS requirements. CIS officers must emphasize to users of this appendix that not all of the listed radio nets will be used in a given operation or exercise. As few as two or three nets may suffice to meet mission requirements.

The kinds of services (voice, video, facsimile, etc.) that are required should be determined and adjusted to conform to available resources (personnel, equipment, and frequency/channel availability) and environmental characteristics. The required service will be governed primarily by the tactical situation, terrain features, and distances between stations on the net (with due consideration to equipment inventories and available personnel). Multiple nets of the same type may be established to handle excess traffic volume. These nets would have a number suffix such as 1, 2, and 3 for the primary, secondary, and tertiary circuits of the same type. The primary net descriptions are given in this appendix.

Within each net composition, units in *italics* normally participate in the specified net as required. There is no absolute requirement for each unit noted to participate in net composition. CIS officers can use the net composition in this appendix for planning and compiling radio guard charts (which SPEED provides) for operations.

Where multiple frequency bands are listed in parentheses following radio net titles, the frequency band that is normally assigned is listed first.

Marine Expeditionary Force Master Net Lists

The MEF Master Net List is a database that facilitates the MEF's Revised Battlefield Electronic CEOI System CEOI generation. These files are unclassified and consist of every circuit within the MEF and each circuit's emission requirements, as well as grouping, call sign, and call word information. The list is important to SINCGARS network planners because it is the sole source for net assignments and net identifiers. Characteristics of the Master Net List are presented in table D-1 (on page D-2).

The MEF Master Net List is controlled by the MEF G-6 and is managed by the MEF frequency manager. The MEF Master Net List will be reviewed annually for proposed modifications on the basis of input from operating force commanders. Requests for modification of the Master Net List will be submitted to higher HQ for consolidation and review. The Master Net List, and thereby CEOI net assignments, should not be modified without the review and approval of the MEF G-6.

The need to maintain consistent, standard radio network terminology demands that MEF radio circuit assignments be regulated. With the introduction of the Revised Battlefield Electronic CEOI System Master Net List, electronic CEOI information can be matched to the task organization, edited, generated, and printed for an entire MEF within hours. Unit participation in Master Net List revisions and compliance are essential to maintaining the currency of this information.

Table D-1. Special Characteristics of the Master Net List.

Item	Purpose	Comment
Net number	Reference	Used to provide task organization requirements to higher HQ
Net name	Description	Standard net description
Net ID	SINCGARS	000 - 999
Call sign	Call-sign assignment	Yes or no, assigned randomly
Organizational code	Echelon separation	Allows for duplicate net IDs within separate units
Restrictions	Subband separation	Allows for restrictive frequency assignments (such as HF day and night)
Frequency	Band assignment	N=None, H=HF, F=VHF, A=VHF-AM, U=UHF, S=SHF, E=EHF
Power	Output power	1-High through 4-Low
Reuse class	Geographic separation	Tactical
Call word	Call-word assignment	Fixed or random

Marine Air-Ground Task Force Command Element Nets

MAGTF CE nets are established to support the exercise of command and control during combat operations. The type operation, commander's intent, concept of operations, environment, enemy capabilities, and MAGTF task organization will influence which nets are required and established. During amphibious operations the term MAGTF is synonymous with the term landing force. MAGTF CE nets follow:

MAGTF Command Net 1 (UHF-SATCOM/HF)

Used to exercise command and coordinate administrative and logistic functions with the major components of the MAGTF.

- CE
- GCE(s)
- ACE(s)
- CSSE
- *Other OPCON units*

MAGTF Tactical 1 (UHF-SATCOM/VHF/HF)

Used to carry operational traffic between the commander and major CEs of the MAGTF.

- CE
- GCE(s)
- ACE(s)
- *Other OPCON units*
- Landing force TACLOG

MAGTF Ground Reconnaissance Command (UHF-SATCOM/HF)

Used for C2 of landing force ground reconnaissance operations and transmission of collected reconnaissance directly to the MAGTF commander or the MAGTF CE combat intelligence center (CIC).

- CE
- OPCON reconnaissance units
- Unmanned aerial vehicle (UAV) squadron/detachment
- *GCE(s)*

- *Other units, as required (e.g., radio battalion radio reconnaissance team (RRT), Navy special warfare teams, etc.)*

MAGTF Alert/Broadcast (HF)

Used for alert warning traffic or general traffic pertaining to all (or the majority) of the units on this net. Messages not of an alert warning type will be consecutively numbered upon transmission.

- CE
- *Designated units within the MAGTF ground element(s)*

MAGTF Intelligence (UHF-SATCOM/HF/VHF).

Used for rapid reporting and dissemination of intelligence, collaborative planning of future MAGTF intelligence operations, and command and control of ongoing MAGTF intelligence and reconnaissance operations.

- CE
- GCE(s)
- ACE(s)
- CSSE
- OPCON intelligence and reconnaissance units
- UAV squadron/detachment

MAGTF Air Observation (UHF/VHF)

Used to coordinate air observation and transmit information from air observers to MAGTF elements. May be used to adjust artillery or naval gunfire (NGF) on an emergency basis.

- CE
- Aerial observer
- GCE
- FSCCs
- *Artillery battery FDC*
- *Supporting arms special staff (SASS)*

MAGTF NGF Support 1 (HF)

Used to request NGF support and coordinate the employment of NGF support ships in general support of the landing force.

- SACC
- GCE(s)
- Landing force general support ships
- *CE*

MAGTF Fire Support Coordination (UHF-SATCOM/VHF/HF)

Used to coordinate all MAGTF fires. Activated at the CE when a FFCC or FSCC is established.

- SACC
- FFCC and senior FSCC(s)
- Senior artillery FDC
- UAV squadron/detachment
- SASS

NGF Control (HF)

Used to request, assign, and relieve fire support ships. Also used to request general support missions and report reliefs, emergencies, and orders pertinent to the execution of scheduled fires. The CATF may establish an NGF control overload net to handle excess traffic.

- CATF/SACC
- Fire support group and unit commanders
- Fire support ships
- Screen commanders
- GCE NGF officer

NGF Ground Spot 1 (HF)

Used to control individual ship gunfire support. Its primary use is to call and adjust fire, and its secondary use is to exchange vital information between stations on the network, such as frontline positions. Activated at the MAGTF CE level when a MAGTF FFCC or FSCC is established.

- Battalion FSCC(s) (NGF liaison officer(s))
- NGF spot team(s)
- FFCC and/or FSCC(s)
- Direct support ship(s)
- General support ship(s)
- UAV squadron/detachment

Shore Fire Control Party Local 1 (VHF)

Used to coordinate shore fire control party activities.

- NGF spot team
- NGF liaison officer

MAGTF Artillery Command/Fire Direction (HF)

Used to direct the fires of artillery units when established ashore. Established only when two or more independent artillery units are providing fire support for the MAGTF.

- FFCC/FSCC/SASS
- SACC (MAGTF artillery officer afloat)
- MAGTF artillery units

MAGTF Artillery Air Spot (UHF/VHF)

Used to conduct air spot for force artillery fires on deep and difficult targets. Activated at MAGTF level only when artillery units are under the direct control of the MAGTF commander.

- Force artillery air spotters
- *CE*
- *GCE artillery air spotters*
- *Artillery units*

MAGTF Convoy Control 1 (VHF/HF)

Used to control the various elements within a convoy. Artillery units and aerial observers may enter to ensure security of motor march routes. Multiple convoy control nets may be required depending on the extent of motor march activity within the force.

- Convoy commander
- Designated convoy elements
- *Artillery units and aerial observers*
- *HQ of unit conducting convoy*

MAGTF Landing Zone (LZ) Control 1 (UHF/VHF)

Used to control and coordinate helicopters en route between the initial point and the LZ.

- MAGTF CE
- Support helicopters
- LZ control team
- MAGTF support party
- Helicopter support teams

Helicopter Support Team Control 1 (HF)

Used to control and coordinate helicopter support team activities.

- MAGTF CE TACLOG group
- TACLOG support helicopters
- MAGTF support party
- Helicopter support teams

Helicopter LZ (HLZ) Local 1 (VHF)

Used to coordinate helicopter support team activities within an LZ.

- Helicopter support team

MAGTF CSS (UHF-SATCOM/HF/VHF)

Used to coordinate CSS within the MAGTF.

- CE
- GCE(s)
- ACE(s)
- CSSE
- TACLOG element

MAGTF Damage Control (HF)

Used to exchange damage assessment information subsequent to an enemy attack with mass destruction means. Also used to direct and coordinate evacuation and casualty assistance for a stricken unit.

- *CE*
- *All MAGTF units of battalion/squadron size and larger*
- *Damage control parties/ monitor teams*
- *Mass evacuation units*
- *Designated medical units*

MAGTF Damage Control Local 1 (VHF)

Used to coordinate damage control efforts within a local area.

- *Damage control parties*

MAGTF Support Party Control (HF)

Used for combat units to request support from the landing force support party (LFSP) and for the LFSP to coordinate with TACLOGs for landing of equipment and supplies.

- Landing force TACLOG
- GCE TACLOG
- MAGTF support party
- LFSP liaison teams
- *FSSG/brigade service support group/MEU service support group*

Shore Party Net (VHF)

Used to coordinate shore party activities on a landing beach or on multiple beaches.

- Shore party
- *Beach party team*

MAGTF Local Security (VHF)

Used to coordinate CE security.

- HQ commandant
- Security elements as directed

MAGTF Medical Regulating (HF)

Used to coordinate casualty distribution among medical treatment facilities.

- Landing force casualty evacuation agency
- Medical battalion/unit
- Hospital ships
- *Designated medical facilities*

MAGTF Communications Information Systems Coordination 1 (UHF- SAT-COM/HF/VHF)

Used to coordinate, install, and restore MAGTF communications-information systems operations.

- CE (G-6/S-6)
- GCE (G-6/S-6)
- ACE (G-6/S-6)
- CSSE (G-6/S-6)
- Communications unit (S-3/detachments)

MAGTF EW Coordination (HF)

Used to coordinate electronic attack (EA) and SIGINT activities.

- CE (G-3/S-3 EWCC)
- OCAC
- GCE
- TACC
- TAOC

MAGTF Defense Special Security Communications System Entry (UHF-SATCOM/HF/Multiplex (MUX))

Used to provide the MAGTF commander with an SCI data communication capability with external agencies. The communication path is provided by the supported commander, and the terminal equipment and personnel are provided by the radio battalion/special security communications team (SSCT).

- MAGTF CE via the radio battalion/detachment special security communication element

MAGTF Special Intelligence Communications Net External (HF)

Used to provide the MAGTF commander with a secure data communications channel for the exchange of SCI. The communications path is provided by the supported commander, and the terminal equipment and personnel are provided by the radio battalion/SSCT.

- MAGTF CE via the radio battalion detachment special security communication element
- CJTF
- CATF

MAGTF Critical Communications (CRITICOMM) Net (UHF-SATCOM/VHF)

Used to provide the supported commander with a channel to adjacent Service cryptologic agencies or cryptologic support group. The communications path is provided by the supported commander, and the terminal equipment and personnel are provided by the radio battalion/SSCT.

- MAGTF CE via the radio battalion/ SIGINT support unit (SSU) special security communications element
- Higher HQ, adjacent HQ, and theater and national intelligence/SIGINT agencies

MAGTF Internal Special Intelligence Communications Handling System Net (VHF/UHF/SHF)

Used to provide the MAGTF commander with a secure SCI communications capability with subordinate division/wing commanders through their organic SSCT. The communications path is provided by the supported commander, and the terminal equipment and personnel are provided by the radio battalion/SSCT.

- MAGTF CE via radio battalion/SSU special security communications element
- Division SSCT

- MAW SSCT

Radio Battalion/SSU Command and Control Net (HF/VHF)

Used to provide the battalion commander/detachment officer in charge with command and control of subordinate elements. The communications path, equipment, and personnel are provided by the radio battalion.

- Radio battalion
- Radio battalion direct support unit

Theater Cryptologic Support Net (HF/UHF-SATCOM)

Used to provide rapid exchange of cryptologic information with the cryptologic elements of other organizations. The communications path is provided by the supported commander, and the terminal equipment is provided by the radio battalion direct support unit.

- MAGTF (radio battalion direct support unit)
- Adjacent Service cryptologic elements
- National cryptologic agencies
- Joint/ATF cryptologic agencies

Radio Battalion CRITICOMM Net (UHF-SATCOM/HF/VHF)

Used to provide CRITICOMM facilities to battalion elements that are physically removed from the CP in support of MAGTF units. The communications path is provided by the supported commander, and the equipment and personnel are provided by the radio battalion.

- Radio battalion
- Radio battalion direct support unit (at least two)

Radio Battalion/SSU Collection and Reporting Net (UHF-SATCOM/HF/VHF)

Used to provide command and control and SIGINT reporting capabilities for battalion/SSU collection operations.

- Radio battalion/SSU (OCAC)
- Deployed collection/direction funding (DF) teams

Radio Battalion/SSU EA Control Net (VHF)

Used to provide the direction and control of radio battalion electronic countermeasures assets. The communications path, equipment, and personnel are provided by the radio battalion.

- Radio battalion/SSU (OCAC)
- Deployed EA teams

Radio Battalion/SSU DF Flash Net (VHF)

Used to provide the DF control station with a means of broadcasting DF flashes to the DF outstations. The communications path, equipment, and personnel are provided by the radio battalion.

- Radio battalion/SSU (OCAC)
- Deployed DF teams

Radio Battalion/SSU DF Report Net (VHF)

Used for DF reporting from DF outstations to DF control. The communications path, equipment, and personnel are provided by the radio battalion.

- Radio battalion/SSU (OCAC)
- Deployed DF teams

DF Data Net (VHF)

Used to exchange DF information between outstations and DF control. The communications path, equipment, and personnel are provided by the radio battalion.

- DF outstations
- DF control

Tactical Receive Equipment and Related Applications Program Data Dissemination System

Used to provide global surveillance information in time for sensor cueing and to provide indications and warning. Data is forwarded from sensor to communications gateways/relays for dissemination to worldwide military users via geosynchronous UHF satellite links. TDDS data sources include national and tactical sensor systems.

- Intelligence agencies
- CIC
- OCAC
- SSES
- ATFIC

On-Board Processor/Direct Downlink

Used to distribute nationally generated data to operational forces and commanders worldwide. The information delivered directly to tactical users can be used to support indications and warning, surveillance, targeting (including OTH targeting), maneuver, execution, and battle damage assessment.

- Intelligence agencies
- CIC
- OCAC
- SSES
- Joint intelligence center

TACINTEL Broadcast Service

Used to provide near-real-time intelligence from an open network of interactive participants by using multiple sensors and sources. The TIBS broadcast uses UHF SATCOM assets for network operation and for the relay of out-of-theater specific information into the tactical users' AOs. TIBS participants include a wide variety of national and Service airborne, surface, and subsurface intelligence platforms.

- JTF, theater, and national intelligence organizations
- MAGTF CE (CIC)

- ATFIC (SSES)

Tactical Reconnaissance Intelligence Exchange System

Used to provide high-accuracy targeting data to multi-Service/joint Services command, control, and intelligence users. The TRIXS network supports full-duplex data and half-duplex voice connectivity between user terminals. It is designed to provide in-time intelligence reports that are focused on high-payoff ground threat targets. It is capable of providing maneuver, threat avoidance, targeting, mission planning, and sensor cueing support to commanders at all echelons. The TRIXS network can accept input from up to five intelligence producers such as the Army Guardrail Common Sensor and Airborne Reconnaissance Low, the Air Force Contingency Airborne Reconnaissance System, and the Navy Story Teller System.

- JTF, theater, and national intelligence organizations
- MAGTF CE (CIC)
- ATFIC (SSES)

TACINTEL Net

Used for transmission and reception of sensitive information sensor data and voice among collection and reporting units and detachments of the radio battalion, the MAGTF, and shipboard facilities, TACINTEL is an automated, high-speed data link.

- JTF, theater, and national intelligence organizations
- MAGTF CE (CIC)
- ATFIC (SSES)

Radio Battalion/SSU Mission Equipment Control Data Link Net (UHF)

Used to control, coordinate, and monitor the mission equipment of the MEWSS. This net is used for internal MEWSS operations and for interface and cooperative operation with the Army intelligence and EW common sensor systems.

- MEWSS internal
- Army Guardrail Common Sensor
- Army Ground-Based Common Sensor
- Army Advanced Quickfix

Radio Battalion/SSU DF Net (UHF)

Used to control, coordinate, and report DF data.

- MEWSS
- OCAC
- Army Technical Control and Analysis Element

Radio Battalion/SSU Tasking and Reporting Net (VHF)

Used to issue taskings/report results

- Team Portable Collection System
- Analyst Subsystem
- Collection outstations

Radio Reconnaissance Command (UHF-TACSAT)

Used for command and control of deployed RRTs; reporting of SIGINT collection and DF reports.

- MAGTF CE (CIC)
- ATFIC (SSES)

TROJAN SPIRIT II Net (C and Ku Band SATCOM)

Used to receive, report, and disseminate intelligence information over a special-purpose satellite system.

- MAGTF CE (CIC/OCAC)
- ATFIC (SSES)
- External intelligence agencies and organizations

Maritime Prepositioning Ships (MPS) Offload 1 (HF/VHF/UHF SATCOM)

Used to control and coordinate the MPS offload.

- Surveillance, liaison, and reconnaissance party (SLRP)

Force Reconnaissance Company Command (HF)

Used to exercise command and coordinate administrative and logistic requests of subordinate units.

- Unit HQ
- Subordinate units
- *Liaison personnel*

Surveillance and Control Data Link (UHF)

The surveillance and control data link is used to transmit moving target indicator, synthetic aperture radar, and fixed target indicator data acquired by Joint STARS to the MAGTF CE to support target acquisition, situation development, battlespace management, and targeting functions.

- JSTARS
- MAGTF CE G-2 section's CGS

Air/Naval Gunfire Liaison Company/ Marine Liaison Group Command (VHF/UHF)

Used to exercise command and coordinate administrative and logistic requests of subordinate units.

- ANGLICO HQ/MLG HQ
- Senior liaison team/Marine liaison companies
- Subordinate liaison teams

Sensor Control and Management Platoon (SCAMP) Command (VHF)

Used for command and control of SCAMP operations and for the coordination of SCAMP administrative and logistic support.

- MAGTF CE CIC (SARC/SCAMP liaison and control element)
- SCAMP/detachment HQ
- Monitoring sites/deployed sensor employment squad (SES)/sensor employment team liaison teams

- *Others, as required*

Sensor Reporting Net (VHF)

Used as a means for rapid reporting of sensor data to supported units.

- MAGTF CE CIC (SARC [net control])
- SCAMP monitoring sites
- Supported units
- *Others, as required*

SCAMP Data Transmission (VHF)

Used for transmission of sensor data collected by remote sensor sites.

- SCAMP liaison and control element monitoring sites
- MAGTF CE CIC (SARC)
- Remote sensor and sensor relay sites

CI/HUMINT Team(s) Command (HF/VHF)

Used for command and control of CI teams and subteams, interrogator-translator teams and subteams, and HUMINT exploitation teams operations and the coordination of CI/HUMINT administrative and logistic support.

- MAGTF CE CIC (SARC HUMINT liaison and control element)
- CI/HUMINT company/detachment HQ
- Deployed CI/HUMINT teams and subteams
- *Others, as required*

CI/HUMINT Reporting Net (VHF)

Used as a means for the rapid reporting of CI/HUMINT data to supported units.

- MAGTF CE CIC (SARC [net control])
- Deployed CI/HUMINT teams and subteams
- Supported units
- *Others, as required*

Ground Combat Element Nets

Division/GCE Command 1 (HF)

Used by the division/RLT/BLT commander to exercise command and coordinate administrative and logistic functions.

- GCE HQ (forward, main, and alternate CPs)
- Artillery regiment/battalion/battery
- Infantry regiment/battalion/company
- Reconnaissance battalion/company/platoon
- LAR battalion/company
- Tank battalion/company/platoon
- Assault amphibian battalion/company/platoon
- Combat engineer battalion/company/platoon
- *GCE TACLOG group*
- *Attached combat and CSS units*

Division/GCE Tactical 1 (UHF-SATCOM/HF/VHF)

Used by commanders to exercise TACON of major combat units of the GCE.

- GCE HQ (forward, main, and alternate CPs)
- Infantry regiment/battalion/company
- Artillery regiment/battalion/battery
- Reconnaissance company/platoon
- LAR battalion/company
- Tank battalion/company/platoon
- Assault amphibian battalion/company/platoon
- Combat engineer battalion/company/platoon
- UAV squadron/detachment
- *Attached combat units*
- *GCE TACLOG*
- *MAGTF TACLOG*

Division/GCE Ground Reconnaissance Company Command (HF/VHF)

Used for command and control of ground reconnaissance operations and for reporting reconnaissance information for deployed reconnaissance elements/teams to the GCE G-2/S-2 (SARC).

- GCE HQ (G-2/S-2/SARC)
- Reconnaissance units
- LAR units
- UAV squadron/detachment

Division/GCE Intelligence (HF/VHF)

Used to provide rapid reporting and dissemination of intelligence, collaborative planning of future intelligence operations, and command and control of ongoing intelligence and reconnaissance operations.

- GCE HQ (G-2/S-2/MAFC)
- Infantry units
- Artillery units
- Reconnaissance units
- LAR units
- Tank units
- Assault amphibian units
- Combat engineer units
- Attached/direct support intelligence units (RadBn SIGINT support unit [SSU], CI team)
- UAV squadron/detachment
- *Attached combat and combat support units*

Marine Division Defense Special Security Communications System Entry (UHF-SATCOM/HF/MUX)

Used to provide the division commander with an SCI data communication capability with external agencies. The communications path is provided by the communications company, and the terminal equipment and personnel are provided by the division SSCT.

- SSCT

Division/GCE Fire Support Coordination (HF/VHF)

Used to provide division/GCE-level fire support coordination.

- GCE FSCC

- Artillery regiment
- Subordinate regiment FSCC(s)
- UAV squadron/detachment
- DASC

Division/GCE Communications Information Systems Coordination 1 (HF/VHF)

Used to coordinate, install, maintain, and restore GCE communications information systems operations.

- GCE HQ (G-6/S-6)
- Infantry S-6s and communications information systems units
- Artillery S-6s and communications information systems units
- *Separate battalions (S-6)*
- *Attached combat and combat support units*

Division/GCE Convoy Control 1 (VHF)

Used to control elements within a convoy and to ensure security (threat and fratricide) of motor march routes.

- Convoy commander
- Convoy elements
- *Artillery units*
- *Aerial observers*
- *Division HQ*

Military Police (MP) Company Command (VHF)

Used to exercise command and to coordinate administrative and logistic functions.

- MP company HQ
- MP units
- *GCE provost marshal*
- *Traffic control/mobile units*

MP Company Tactical 1 (VHF)

Used by MP commander to tactically control and coordinate MP activities.

- MP company HQ
- MP units
- Traffic control/mobile units

Combat Engineer Battalion Command (HF)

Used for administrative control and OPCON of subordinate units.

- Combat engineer battalion HQ
- Engineer units
- *Supporting and attached units*
- *Liaison personnel at higher HQ*

Engineer Company Command (VHF)

Used for administrative control and OPCON of subordinate units.

- Engineer company HQ
- Engineer units
- *Liaison personnel at higher HQ*

Engineer Local (VHF)

Used to coordinate engineer efforts within a local area.

- *Engineer units/detachments*

Tank Battalion/Company/Platoon Command 1 (VHF)

Used to exercise command and coordinate administrative and logistic requests. Separate command nets are set up for each echelon in the battalion. Separate tube-launched, optically tracked, wire command link guided missile (TOW) company, platoon, and section command nets are also included.

- Tank battalion/company/platoon HQ
- Tank companies/platoons/tanks
- Tank recovery on tank company command
- TOW companies, platoons, sections, squads
- *Liaison personnel*
- *Supporting and attached units*

LAR Battalion/Company/Platoon Tactical 1 (VHF/HF)

Used to exercise TACON of subordinate units. Each echelon has its own tactical command (TAC) net.

- Unit HQ
- Subordinate units and vehicles
- Recovery vehicles (company net)
- Liaison personnel
- Attached units

LAR Battalion Command (HF/VHF)

Used to exercise command and coordinate administrative and logistic support.

- Battalion HQ
- Companies
- Liaison personnel
- *Supporting/attached units*

LAR Battalion Mortar (VHF)

Used to request and control the fires of the mortar platoon.

- Forward observer teams
- Mortar platoon FDC
- Mortar representative at the battalion HQ

Assault Amphibian Battalion/Company/Platoon Command (VHF).

Used to exercise command and coordinate administrative and logistic support. Each echelon has its own command net.

- Unit HQ
- Subordinate units/vehicles
- Recovery vehicles (company net)
- *Liaison personnel*

Reconnaissance Company/Platoon Command (HF/VHF)

Used to exercise command and coordinate administrative and logistic support.

- Unit HQ
- Subordinate units
- Patrols/support aircraft/vehicles
- *Supporting units*
- Liaison teams at supported units

Infantry Regiment Command (HF)

Used to exercise command and coordinate administrative and logistic support.

- Infantry regiment HQ
- Infantry battalions
- CSS area HQ
- *Landing support company*
- *Attached units*

Infantry Regiment Tactical 1 (VHF)

Used to exercise TACON of subordinate units.

- Infantry regiment HQ
- Infantry battalions
- *Regimental TACLOG*
- *Supporting and attached units*

Infantry Regiment Intelligence (VHF)

Used for rapid reporting and dissemination of intelligence, collaborative planning of future intelligence operations, and command and control of ongoing intelligence and reconnaissance operations.

- Infantry regiment HQ
- Infantry battalions
- Intelligence units (radio battalion SSU, counterintelligence team)
- *Supporting and attached units*
- *Regimental observation post*

Infantry Regiment Fire Support Coordination (VHF)

Used for regimental-level fire support coordination.

- Infantry regiment FSCC
- Infantry battalion FSCC(s)
- Artillery battalion(s)
- *Other supporting HQ*

Infantry Regiment Communications Information Systems Coordination (VHF)

Used to coordinate, install, maintain, and restore regimental communications-information systems operations.

- Infantry regiment HQ
- Infantry battalions
- *Supporting and attached units*

TACP Local (VHF)

Used to coordinate activities of the air liaison officer and forward air controllers.

- Air liaison officer
- Forward air controllers

Infantry Regiment Local Security (VHF)

Used to coordinate HQ main area, rear area, and CP security elements. Multiple security nets will be required.

- HQ commander
- Security elements

Infantry Battalion Tactical 1 (VHF)

Used to exercise tactical control and fire direction of subordinate units.

- Infantry battalion HQ
- Rifle companies

- *Weapons company*
- *Battalion TACLOG group*
- *Landing support or helicopter support teams*
- *Battalion liaison officer(s)*
- *Supporting and attached units*

Infantry Battalion Mortar (VHF)

Used to request and control the fires of the 81-mm mortar platoon.

- Forward observer teams
- 81-mm mortar platoon FDC
- 81-mm mortar representative at battalion HQ

Scout-Sniper Command (VHF)

Used to exercise command and control of battalion scout-sniper operations and to report reconnaissance information collected by deployed scout-sniper teams.

- Battalion S-2 and S-3 (fires)
- Scout-sniper teams

Rifle Company/Platoon Tactical (VHF)

Used to exercise TACON of subordinate units.

- Rifle company or platoon HQ
- Rifle platoons or squads/fire teams
- Weapons platoon or sections
- *Company or platoon observation posts*
- *Supporting and attached units*

Artillery Regiment/Battalion/Battery Command 1 (HF, Regiment; VHF, Battalion/Battery)

Used to exercise command and coordinate administrative and logistic requests. May be used as an alternate fire direction net.

- Artillery unit HQ
- Subordinate artillery units
- Attached/reinforcing artillery units
- *Division HQ*

Artillery Regiment Tactical 1/2 (VHF/HF)

Used as a supplemental means for the commander to exercise command and control of subordinate units when the command and fire direction nets become overloaded. This net may also be used by the artillery battalion liaison officers for the rapid exchange of fire planning data, counterfire information, and other artillery liaison activities.

- Artillery regiment HQ
- Division HQ (forward, main, alternate CP)
- Artillery battalions
- Attached artillery units
- *Supporting artillery units*
- *Artillery battalion liaison officers*

Artillery Regiment/Battalion/Fire Direction 1/2 (VHF/HF, Regiment; VHF, Battalion)

Used to exercise tactical fire direction of subordinate units by the assignment of fire missions, designation of units of fire, and conduct of time-on-target missions. Subordinate units may use this net to request additional fires from organic and attached artillery units. This net may also be used for the exchange of infantry fire planning data and fire support coordination information when no other means is available.

- Artillery unit HQ
- Division FSCC
- Subordinate artillery units
- Attached/reinforcing artillery units
- Supporting artillery units
- Artillery liaison officers

Artillery Regiment Communications Information Systems Coordination (VHF/HF)

Used to coordinate installation and restoration of communications-information systems capabilities.

- Artillery regiment HQ

- Artillery battalions

Artillery Regiment Radar Telling (VHF)

Used to exchange radar intelligence information and for requests for surveillance of enemy counterfire weapons. May also be used for registration and adjustment of artillery fire.

- Artillery regiment HQ
- Countermortar radar sites
- *Artillery battalions and batteries*

Artillery Regiment Survey/Metro (VHF)

Used to exchange survey, meteorological, and ballistic information and data between survey teams and artillery units.

- Artillery regiment HQ
- Artillery battalions/batteries
- Survey officers and teams
- *Division HQ*

Artillery Battalion/Battery Conduct of Fire (VHF)

Used by forward observers to request and adjust artillery fire. Established when fire direction is centralized; when fire direction is decentralized, each battery in the battalion has a separate conduct-of-fire net that terminates at the battery HQ. There may be as many as four conduct-of-fire nets in each direct-support artillery battalion.

- Artillery battalion or battery HQ
- Battery forward observers
- Battery liaison officers
- UAV squadron/detachment
- *Artillery battalion liaison officers*
- *Attached/reinforcing artillery units*

Aviation Combat Element Nets

Wing radio nets that are replaced by static MUX circuits will remain available as backups.

ACE Command Net 1 (HF)

Used to exercise command and coordinate administrative and logistic support.

- ACE HQ
- MAGs
- Marine wing support group/squadron
- Marine air control group/detachment
- Independent squadrons/battalions
- *Attached units*

Tactical Air Command 1 (UHF-SATCOM/HF)

Used by the tactical air commander to task subordinate elements to provide aircraft for missions.

- TACC/tactical air direction center (TADC)
- TAOC(s)
- DASC
- Marine aircraft groups/squadrons (as required)
- *MATCDs*
- *Early warning/control (EW/C)*

Command Action (HF/VHF/MUX)

Used for command-level coordination of anti-air warfare (AAW) through the exchange of information pertaining to missile battery employment, assignment of air targets, and the interceptor/missile coordination. Net functions may be performed over the air operations control net when an MCR circuit is not established.

- TACC/TADC
- TAOC(s)
- EW/C

Antiaircraft Control (HF/VHF/MUX)

Used to control surface-to-air missile (SAM) batteries. Types of information passed on this net include: target assignments, fire direction orders, weapons status commands, battery status reports, and progress-of-engagement reports.

- TAOC(s)

- EW/C
- LAAD Battery CP/ADCP

Air Operations Control (HF/MUX)

Used by TAOC to request interceptor aircraft and report friendly air defense situation information to the TACC/TADC. Used to exchange information pertaining to combat air patrol availability, stationing and assignment, assignment and disposition of targets, intercept progress, SAM unit status and employment, and aircraft/missile weapons coordination. Multiple air operations control nets are normally required; one or more for each TAOC in operation.

- TACC/TADC
- TAOCs
- LAAD Battery CP/ADCP
- *Early warning/control activities*

Antiaircraft Intelligence (HF/MUX)

Used by SAM batteries to report targets acquired by the battery surveillance radar. TAOC passes selected early warning contacts to missile firing units. Combined with the antiaircraft control net when MUX is not available.

- TAOC(s)
- Air defense fire units
- EW/C
- LAAD Battery CP/ADCP

Combat Information/Detection (HF/MUX)

Used to report unidentified or hostile aircraft, including initial contact reports, tracking, amplifying, and final disposition. Multiple combat information/detection nets may be established for multiple TAOCs.

- TAOC(s)
- Early warning/control activities
- LAAD Battery CP/ADCP
- Air defense fire units
- DASC (as required)

- MATCD (as required)
- *TACC/TADC*
- *Other reporting agencies*

Handover/Cross Tell (HF/MUX)

Used to transfer aircraft control between air control agencies. Multiple nets can be established for the TAOC-early warning/control handover or ground control intercept-ground control approach handover. Functions may be combined on one net if traffic permits.

- *TAOC*
- *Early warning/control*
- *ATC Detachment, MACS*
- *MATCD*
- *Other-Service control agencies*

LAAD Battalion Command (HF)

Used to exercise command and coordinate administrative and logistic support.

- LAAD battalion HQ
- LAAD battery
- Command Posts/ADCP

LAAD Weapons Control (HF)

Used for air defense warnings, weapons control conditions, and pertinent information concerning friendly, enemy, or unknown aircraft.

- Command Posts/ADCP
- LAAD battery
- LAAD platoon commanders/section leaders

LAAD Team Control (VHF)

Provides air defense warnings, weapons control condition and pertinent information concerning friendly, enemy, or unknown aircraft to LAAD teams. Multiple LAAD team control nets are normally employed.

- LAAD section leaders
- LAAD teams

Interface Coordination (HF/UHF VHF/MUX)

Provides a means for command level coordination in the employment of certain tactical weapons and for interface command, control, and coordination.

- TACC
- Other-Service agencies
- *TAOC*

TADIL A (HF/UHF)

Used to exchange digital data between various TDSs. Types of data passed include air and surface tracks, weapons status, and selected orders and functions. TADIL A operates as a star-netted data link.

- TACC
- TAOC(s)
- EW/C
- *Other-Service air control agencies*

TADIL B (MUX)

Used in a point-to-point mode by using a full-duplex wire/multichannel path (a functional equivalent to TADIL A). NATO designation: Link 11 B.

- TACC
- TAOC(s)
- EW/C
- MATCD
- *Other-Service air control agencies*

TADIL C (UHF)

Used as a one- or two-way unsecure digital data link between air control agencies and interceptor aircraft. NATO designation: Link 4A.

- TAOC
- EW/C
- Interceptor aircraft
- *Other-Service air control agencies (E-3/E-2C aircraft, ship AAW facilities)*

Army Tactical Data Link (ATDL)-1 (MUX)

Used for secure, point-to-point exchange of air breathing track data. Data passed includes reference tracks, missile status, and missile engagements.

- TAOC
- Early warning/control
- Army Air Defense units

Ground-Based Data Link (VHF)

Used for air defense CP downlink of surveillance information to short-range firing units.

- ADCP
- Short-range air defense
- Remote sensors

Point-to-Point Data Link (MUX)

Used for one-way transmission of TBM nonair breathing track data.

- ADCP
- TPS-59 radar

Track Supervision Net (TSN) (HF/UHF/MUX)

Used by surveillance personnel to exchange information in order to maintain a clear picture. May be combined with Data-Link Coordination Net (DCN) for SCR operations.

- TACC/TADC
- TAOC(s)
- Antiaircraft operations center
- Early warning/control activities

Data-Link Coordination Net (HF/UHF/MUX)

Used for maint/coord of data-link operation. May be combined with TSN for SCR operations. Generally one DCN per TADIL-B/ATDL-1.

- TACC
- TAOC
- *Other-Service air control agencies*

Radar Remote Coordination (VHF/HF)

Used to exchange early warning/control track and control data.

- TAOC
- TAOMs
- Early warning/control sites

Voice Product Net (HF/UHF/MUX)

Used to report/forward hostile target SIGINT information that is not reportable in a standard data format.

- TACC
- TAOC
- *Other interfacing agencies*

ACE Communications Information Systems Coordination (HF/VHF)

Used to coordinate installation and restoration of communication capabilities.

- Wing HQ
- Marine aircraft groups
- MACGs
- Marine wing support group/squadron
- Independent squadrons/battalions
- *Attached units*

Direct Air Support (HF/MUX)

Used by DASC to request direct air support aircraft from the TACC. Information pertaining to aircraft stationing, fuel and ordnance status, and progress of direct air support missions may be passed over this net.

- TACC/TADC
- DASC

Tactical Air Request/Helicopter Request (TAR/HR) (UHF-SATCOM/HF/VHF)

Used by forward ground combat units to request immediate air support from the DASC. Intermediate ground combat echelons (FSCCs) monitor this net and may modify or disapprove a specific request. The DASC uses the net to brief the requesting unit on the details of the mission. Target damage assessments and HRs may be passed over this net. Multiple TAR/HR nets may be required, depending on the scope of close air support operations.

- DASC
- TACPs
- HDC
- TAOC
- *Tactical air coordinator (airborne)*
- *Forward air controller (airborne)*

Tactical Air Traffic Control (TATC) (UHF/VHF)

Used by the TACC/TADC, TAOC, and DASC to exercise control of all tactical and itinerant aircraft in the objective area. Used to pass aircraft reports of launches by mission number, to clear aircraft to their assigned control agencies, to divert aircraft as necessary, and to report missions completed before landing. Multiple TATC nets are required for each control agency.

- TACC/TADC
- TAOC(s)
- DASC
- EW/C
- Fixed-wing aircraft
- Helicopters
- UAV ground control station (GCS)

Fighter Air Direction (FAD) (UHF/VHF)

Control aircraft in the conduct of intercepts. Multiple FAD nets are required and assigned to major control agencies.

- TAOC
- Early warning/control
- Interceptor aircraft
- Other-Service AAW agencies

Tactical Air Direction (TAD) (UHF/VHF)

Used to direct aircraft in the conduct of offensive air support missions and to brief support aircraft on target information or assignment. Multiple TAD nets are required and are assigned to major air control agencies by the DASC. This net is primarily UHF with a secondary VHF capability available in some cases.

- DASC
- UAV GCS
- TACP
- *Forward air controller (airborne)*
- *Offensive air support aircraft*

Helicopter Direction (HD) (UHF/VHF/HF)

(Navy: inbound and outbound; USMC: control of helicopters in the objective area) Used by the HDC for positive control of inbound and outbound helicopters in the amphibious objective area. The radar controller in the HDC uses these nets to direct flight course and altitude of helicopters and holdings, let-downs, and climbout when required. Both UHF/VHF and HF HD nets are employed. Multiple HD nets are required and are allocated by the DASC.

- DASC
- HDC
- UAV GCS
- *Assault support coordinator (airborne)*
- *Helicopters*
- *Helicopter LZ Control Team (LZCT)*
- *Tactical air controller (airborne)*
- TACP

Tanker (UHF)

Used by in-flight refueling aircraft to communicate with the tanker. Used by TAOOC to exchange information with the tanker.

- Tanker
- In-flight refueling aircraft
- EW/C
- TAOOC

Squadron Common (UHF/VHF)

Used for in-flight group or squadron aircraft, and group or squadron HQ, communications. Each aircraft squadron has its own common net.

- Group or squadron HQ
- *In-flight group or squadron aircraft*

Guard (UHF/VHF/HF)

Used by aircraft to declare an emergency. Used by air control agencies to advise aircraft of emergency conditions or serious hazards to aircraft safety.

- TACC/TADC
- TAOOC(s)
- DASC
- MATCD
- EW/C
- Fixed-wing and helicopter aircraft

Crash, Fire, and Rescue (VHF)

Used to coordinate crash recoveries on or around an airfield.

- Crash crew
- ATC facility
- Airfield operations
- Explosive ordnance disposal
- Medical facility
- MP

Search and Rescue (SAR) (UHF/VHF)

Used to control and coordinate air rescue missions. Multiple SAR nets may be required depending on the number of concurrent SAR missions.

- *All elements within the command and control system*
- Aircraft involved in SAR missions

ATC Common (HF/MUX)

Used to coordinate airspace management between airfields.

- Air traffic controller(s)

Approach Control (UHF/VHF)

Used to control air traffic approaching the terminal airspace.

- Approach controller
- Approaching aircraft

Departure Control (UHF/VHF)

Used to control air traffic departing the terminal airspace.

- Air Traffic Control Facility
- Departing aircraft

Ground Control Approach (GCA) (UHF/VHF)

Used to provide bearing and altitude to approaching aircraft.

- TATC
- Aircraft

Ground Control (UHF/VHF)

Used to control ground movement of vehicles, aircraft, and personnel on the taxiways and runways.

- Ground control
- Aircraft
- Vehicles
- Personnel

LZ Control (VHF/UHF)

Used to control aircraft en route between the initial point and the LZ.

- LZCT
- Aircraft en route between the initial point and the LZ
- *DASC*
- *Aircraft coordinator (airborne)*

LZCT Local (VHF)

Used to direct the activities of aircraft control personnel in each of the landing sites.

- LZCT commander
- Landing site controllers

Air Base Security (VHF)

Used to coordinate security operations of expeditionary airfields (EAFs).

- MPs at the EAFs

Air Defense Alert (UHF)

Used to direct coordination and exchange of critical threat information and verbal warning to aircraft transiting minimum risk routes and operating near missile engagement zones.

- Ground-based air defense units
- Combat air patrol aircraft
- Transiting to friendly aircraft

Convoy Control (VHF)

Used to control the various elements within a convoy.

- Convoy commander

- Convoy elements
- Aerial observers
- ACE HQ

Defense Meteorological Satellite Program Satellite Imagery (SATCOM)

Used as an encrypted receive-only circuit to provide a direct readout of real-time satellite imagery from polar orbiting satellites of the Defense Meteorological Satellite Program.

- Deployed Marine wing support squadron (MWSS)

Fire Support Safety (HF)

Used to exchange information concerning the employment of artillery, NGF, surface-to-surface missiles, and close air support aircraft to ensure safety of all aircraft in the objective area.

- Air control agencies and elements

Fleet Facsimile (HF)

Used as a broadcast receive-only circuit to provide weather graphics produced by Navy regional centers.

- Broadcast from NCTAMS
- Deployed MWSS

Fleet Multichannel Broadcast (UHF SATCOM)

Used as a receive-only circuit on channels 8 or 15 (environmental channels) of the satellite to provide weather bulletins produced by Navy regional centers.

- Broadcast from NCTAMS
- Deployed MWSS

Goldwing Communications (HF)

Used as a secure, in-theater, joint net that may be used for voice traffic but is primarily for transmitting and receiving alphanumeric weather data.

- Other-Service meteorological and oceanographic agencies
- Deployed MWSS

Landing Signal Officer (UHF)

Used to coordinate control of the landing pattern with the control tower and to control aircraft in the landing pattern. A tower secondary frequency is normally used for this requirement.

- ATC Facility
- Aircraft in pattern
- Landing signal officer

Medical Evacuation (MEDEVAC) Coordination Net (VHF)

Used to coordinate MEDEVACs.

- Requesting unit
- Evacuation helicopters
- Medical facilities

Pilot to Metro (UHF)

Used for exchange of meteorological information.

- Flying aircraft
- Weather detachment at EAF

Rear Area Security (VHF)

Used to coordinate security operations of groups/squadrons/attached units at EAFs and air control agency locations.

- Security element task organized by the units at the EAFs and air control agency locations

Strip Alert (HF/VHF)

Used to coordinate fixed-wing aircraft and helicopter operations at the EAF.

- Air boss
- Tactical air watch officer

- Assault support watch officer

Tactical Alert (HF)

Used for rapid dissemination of air-raid warnings.

- MAGTF HQ
- GCE/ACE/CSSE HQ
- Air control agencies

Television Infrared Observation Satellites Imagery (SHF)

Used as an unencrypted receive-only circuit to provide a direct readout of real-time satellite imagery from the National Oceanographic Atmospheric Administration.

- Deployed MWSS

Tower Hot (HF/VHF)

Used by ATC to inform the TACC of launched aircraft.

Tower Primary (UHF/VHF)

Used by controller to issue traffic advisories and aircraft clearances within the EAF.

Tower Secondary (UHF/VHF)

Overflow traffic from the tower primary.

Weather Radar Net (AN/FPS-106)

Used as a single-site radar that provides a visual depiction of precipitation and storm structure within a 200-nautical-mile radius of its location.

- Deployed MWSS at the EAF

Wing Intelligence (HF)

Used for rapid reporting and dissemination of intelligence information.

- ACE G-2
- Group S-2
- Squadron S-2

MAW Defense Special Security Communications System Entry (UHF-SAT-COM/HF/MUX)

Used to provides the wing commander with an SCI data communication capability with external agencies. The communications path is provided by the communications company, and the terminal equipment and personnel are provided by the MAW SSCT.

- SSCT

Wing Logistic Net (HF)

Used to request logistic support.

- ACE G-4
- Group S-4
- Squadron S-4

Link-1 (NATO) (MUX)

Used for point-to-point interface with NATO Air Defense Ground Environment (NADGE) agencies in a full-duplex data link to exchange air defense information.

- TACC/TADC
- TAOC
- NADGE agencies

UAV Command Net (HF/VHF/UHF)

Used to coordinate UAV activities.

- UAV squadron/detachment HQ
- GCS
- Launch and recovery site
- Remote video terminal teams

UAV Primary Uplink Control (G-Band)

Used to control air vehicle and payload.

- Ground data terminal
- Launch and recovery
- Air vehicle

UAV Secondary Uplink Control (G-Band)

Used to control air vehicle and payload if primary link control is lost.

- Ground data terminal
- Launch and recovery
- Air vehicle

UAV Telemetry Downlink (G-Band)

Used to provide real-time video display of target area and downlink flight control data.

- GCS
- Launch and recovery site
- Remote video terminal teams
- Air vehicle

Combat Service Support Element Nets

CSS Command 1/2 (UHF-SATCOM HF/VHF)

Used to exercise command and coordinate administrative and logistic support.

- Unit HQ
- General support group
- Direct support group
- CSS detachments

CSS Alert/Broadcast (HF)

Used for alert warning or general traffic pertaining to all (or a majority) of the units. Messages not of an alert warning type will be consecutively numbered at the time of transmission.

- Unit HQ
- General support group
- Direct support group
- CSS detachments

CSS Damage Control (HF)

Used for damage assessment information that is exchanged subsequent to an enemy attack with mass-destruction means. Evacuation and casualty assistance for stricken units may also be directed over this net.

- Unit HQ
- General support group
- Direct support group
- CSS detachments

CSS Communications Information Systems Coordination (HF/VHF)

Used to coordinate, install, maintain, and restore CSSE communications and information systems operations.

- Unit HQ
- General support group
- Direct support group
- CSS detachments

CSS Local (VHF)

Used to coordinate activities within CSS local area.

- Unit HQ
- General support group
- Direct support group
- CSS detachments

CSS Security (VHF)

Used to coordinate security elements in the CSS operating areas.

- CSS HQ commandant
- Security elements as directed by HQ commandant

CSS Request (UHF-SATCOM/VHF)

Used to receive requests from supported units and provide status.

- CSSOCs

- CSS detachments
- Supported unit(s)

LFSP Command (HF/VHF)

Used to exercise command and coordinate administrative and logistic support of own units. This net is also used to coordinate the movement of supplies being landed over multiple colored beaches.

- LFSP HQ
- Shore party/helicopter support groups
- *Shore party/helicopter support team*

Shore Party Control (VHF/HF)

Used to coordinate the flow of supplies and personnel. A separate net is established for each color of beach.

- Shore party group (operating the beach)
- Shore party teams
- TACLOG group of supported units using indicated beach
- Shore party liaison teams with supported units
- *LFSP HQ*
- MAGTF TACLOG

Engineer Support Battalion Subordinate Unit Command (HF)

Used to exercise command and coordinate administrative and logistic requests of subordinate units.

- Unit HQ
- Subordinate units

Motor Transport Battalion Company Command/Convoy Control (VHF/HF)

Used to exercise command and coordinate administrative and logistic requests of subordinate units. Used to control and coordinate convoys.

- Unit HQ
- Convoy commander

- Convoy front
- Convoy rear

Medical Battalion Command (VHF)

Used to exercise command and coordinate administrative and logistic requests of subordinate units.

- Medical battalion HQ
- Medical companies
- Hospital companies

Medical Battalion Evacuation Coordination (Ground) (VHF)

Used to coordinate ground MEDEVAC.

- Medical unit HQ
- MEDEVAC ambulances/vehicles
- Evacuation/treatment facilities
- Requesting units

Medical Battalion Evacuation Coordination (Air) (VHF)

Used to coordinate air MEDEVAC.

- Medical unit HQ
- MEDEVAC aircraft
- DASC
- Evacuation/treatment facilities
- Requesting units

Appendix E

Information Systems Directory

Section I

Overview

An information systems directory is one of the most critical documents pertaining to CIS planning. It shows a subscriber how to use the system to the maximum extent possible without assistance from communications or data systems personnel. The principal function of this directory is to provide guidelines from which CIS officers and telephone systems officers may produce a directory for their commands/organizations. Section II of this appendix is a sample directory for II MEF. It supports the design characteristics of the MAGTF tactical communications network.

Security of Information

The information systems directory for a given organization, even one as large as the MEF, need not be classified if the directory contains information derived from unclassified sources. For example, a listing of organizations with subscriber numbers that are consistent with this appendix and are unchanging from operation to operation need not be classified. However, an information systems directory could be used as a source of information for enemy intelligence collection. Therefore, an information systems directory should be handled as For Official Use Only if it contains CIS architecture diagrams or if it will be used in an operation outside of CONUS.

Cover

A cover can specify which organization created the directory, for what community of users the directory is intended, and the effective period for the directory.

Emergency Numbers

Emergency numbers provide the subscriber rapid access to the numbers of certain critical agencies (e.g., aid station, combat operations center, force protection platoon). These numbers should also be listed in the organizational listing.

Index

An index is an optional feature that serves as a table of contents. The size of the directory determine the need for an index.

General Instructions

These instructions discuss the differences in the types of telephone equipment that may be used by a unit during an operation. The telephone equipment should include tactical equipment such as the KY-68, TA-954, and TA-1042, STU-III's, commercial equipment, and cellular telephones. Each has its own special operating instructions.

Operating Instructions

These instructions tell subscribers how to effectively use the tactical automated switching system (TASS) and commercial systems. They should list the unique operating characteristics of each telephone system.

Dialing Instructions

These instructions will aid subscribers in using the different telephone systems found in a MEF-level exercise. Instructions should give enough

detail to allow unfamiliar subscribers to effectively use the system. Instructions should not change too much from unit-to-unit or from operation-to-operation, as the equipment characteristics do not change. Instructions do not describe every available subscriber feature of the switching system. This technical information may be found in TMs or the CJCSM 6231 series for the specific equipment.

Precedence Subscribers

Circuit switched calls within a network are processed according to five levels of precedence. The precedence levels follow in ascending order.

Routine (R)

Routine has no precedence over any other call and is handled sequentially as placed by the calling party. There is no preemption of any lines. Routine precedence designation applies to normal official government communications.

Priority (P)

Priority has precedence over any other telephonic call of lower precedence (routine calls). Priority precedence is reserved generally for telephone calls by parties requiring expeditious action or requiring essential information for conducting government operations.

Immediate (I)

Immediate has precedence over and will preempt routine and priority calls. Immediate precedence is reserved generally for telephone calls pertaining to—

- Situations that gravely affect the security of national and allied forces.
- Reconstitution of forces in a post attack period.
- Intelligence essential to national security.
- Diplomatic negotiations to reduce or limit the threat of war.
- Implementation of Federal Government actions essential to national survival.

- Situations which gravely affect the internal security of the United States.
- Civil Defense actions concerning direction of our population and their survival.
- Disasters or events of extensive seriousness having an immediate and detrimental effect on the welfare of the population.
- Vital information having an immediate effect on aircraft, spacecraft, or missile operations.

Flash (F)

Flash has precedence over and preempts immediate, priority, and routine calls. Flash precedence is reserved generally for telephone calls pertaining to—

- Command and control of military force essential to defense and retaliation.
- Critical intelligence essential to national survival.
- Conduct of diplomatic negotiations critical to the arresting or limiting of hostilities.
- Dissemination of critical civil alert information essential to national survival.
- Continuity of Federal Government functions essential to national survival.
- Fulfillment of critical United States internal security functions essential to national survival.
- Catastrophic events of national or international significance.

Flash Override (FO)

Flash override has precedence and preempts all other types of telephone calls. The application of the FO capability is available to—

- The President of the United States, Secretary of Defense, and Joint Chiefs of Staff.
- Commanders of unified and specified commands when declaring either Defense Condition One or Defense Emergency.
- CINCNORAD when declaring either Defense Condition One or Air Defense Emergency and other national authorities as the President may authorize.

Dialing Precedence Calls

The precedence indicator (P, I, F, or FO) is dialed from the subscriber's telephone terminal keypad, and is dialed first in any dialing sequence. If no precedence is dialed, the call is processed as routine. The unit CIS officer (in accordance with standard operating procedures) determines which telephones will have precedence capability. The precedence capability is programmed into the circuit switch memory. If a subscriber has a precedence capability, any precedence indicator can be chosen in a dialing sequence, up to the level that has been authorized. A subscriber attempting to use precedence levels higher than that authorized will have the call processed at the maximum authorized level. Both loops and trunks are preemptable. A call cannot preempt a loop or trunk in the switch that is handling a call of equal or higher precedence.

Numbering Plan

The tactical telephone numbering plan is based on a 13-digit numbering scheme and is structured into four parts:

9YX	MYX	PRSL	GXX
NATO Code	Area Code	Switch Code	Subscriber Number
G = 1–8		PR = 32–39	
M = 2–8		SL = 00–99	
X = 0–9			
Y = 0–1			

NATO Code (9YX)

NATO members have reached a standardization agreement (STANAG) to use a unique three-digit national identification (NI) number. The NI code for tactical U.S. forces is 914. Calls to NATO subscribers can only be made from the medium unit level switch (AN/TTC-42) when it is connected to the AN/TTC-39 large circuit switch.

Area Code (MYX)

An area code is a number that identifies an area or region of switches. Area codes are only assigned during very large military operations in which several Services are working together in a joint operation. DISA DSN area codes are assigned by geographical areas as follows:

- 312 - CONUS
- 313 - Caribbean
- 314 - Europe
- 315 - Pacific
- 317 - Alaska
- 318 - CENTCOM

Unique Area Codes

If a very large military operation is conducted, all of the forces in a theater might be assigned their own unique area code (300 for example). Depending on which part of the world they are deployed to, if a military operation becomes extremely large, the MARFORs have several area codes reserved for their use.

MARFOR ACOM	204
MARFOR CENTCOM	304
MARFOR PACOM	804
MARFOR SOCOM	408

Inter-Area Dialing

When calling a subscriber who is serviced by a different area code (MYX), the full ten-digit number must be dialed (MYXPRSLGXX). As with dialing another PRSL, the same 9 or 91 escape code must be used. The number dialed will be either—

9 MYX PRSL GXX
or
91 MYX PRSL GXX

Switch Code (PRSL)

A switch code is a unique number that identifies one particular circuit switch. It is composed of two parts; the first two digits are the primary zone (PR) and the last two digits are the switch locator (SL). The switch code is also called the "PRSL". All circuit switches must be assigned a switch code, whether operating independently or as part

of a circuit switched network. A four-digit PRSL switch code within a network is also called a 4/3 numbering plan, since the switch code is four digits and the subscriber number is three digits. The 4/3 numbering plan is preferred in military circuit switched systems since it allows for more circuit switches with fewer subscribers as compared to a commercial switching system which uses a 3/4 numbering plan. A commercial switching system has fewer switches with more subscribers, hence the 3/4 code.

Interswitch Dialing

When calling a subscriber who is serviced by a different circuit switch (PRSL), the full seven-digit number must be dialed (PRSL-GXX). But first, the circuit switch must be told that the numbers dialed are PRSL numbers and not subscriber numbers. This is done with a one or two digit special “long-distance” or escape code. Some circuit switches require a “9” or a “91” code prior to the seven digit subscriber number. This is analogous to dialing a “1” for long distance on a telephone at home or in the office. The number dialed will be either—

9 - PRSL - GXX
or
91 - PRSL - GXX

PRs will be assigned by the higher headquarters J6/G-6, according to the Global Block Numbering Plan (GBNP) matrix found in CJCSM 6231.02. Some higher level switches in the military can use a 3/4 numbering plan, which uses a three-digit switch code (NNX) called a local exchange code, vice a PRSL code. The full subscriber number then takes on the form NNXGXXX.

Subscriber Number (GXX)

The subscriber number is a three-digit number between 100 and 899. Every telephone instrument that is connected to a circuit switch, whether automatic or manual, must be assigned a number. All

subscriber numbers are listed together in the information systems directory, which is published by the unit CIS officer prior to an operation. When one subscriber wishes to call another subscriber who is on the same circuit switch, he only needs to dial the subscriber number (GXX).

Global Block Numbering Plan

The Marine Corps will begin using the GBNP in FY 99 to incorporate all of its switches into a joint network. The GBNP will identify all of the services with a unique, service-managed block of numbers, simplify network management into a global network, ensure nonduplication of numbers within an area of responsibility, and identify databases and subnetworks within the assigned block of numbers. After implementing the GBNP, it is expected that a block of numbers (PRSL numbers between 3200–3900) will be associated with each major subordinate command (MSC) and switch type. MSCs should coordinate with their respective preaffiliation managers to determine their subscriber numbers.

LAN Instructions

These instructions address how to use the secured (SIPRNET) and unsecured (NIPRNET) LAN. Instructions should describe all LAN services available, including electronic mail, Internet access, message dissemination, and COMPUSEC.

Information Systems Listing

This listing provides tactical, commercial, DSN, host nation, pager, and cellular telephone numbers for subscribers at every organizational location. It also provides subscriber's SIPRNET and NIPRNET LAN addresses and any operational webpage addresses. The listing should include adjacent major organizations of other services in a joint operation.

Section II

Sample II MEF Information Systems Directory

This section contains a representative information systems directory designed according to the principles outlined in section 1. This sample directory used II MEF as the notional unit. The directory, however, may not accurately reflect the actual composition of the present II MEF, nor does it list all of the potential subscribers to the system. CISOs should consult with the GBNP and their unit's T/Os and SOPs before preparing a directory to ensure that subscriber numbers are accurate.

CLASSIFICATION

II MEF EXERCISE INFORMATION SYSTEMS DIRECTORY

Effective Date 210800Z October XXXX

EMERGENCY NUMBERS

Operator	000
Combat Operations Center	3420-300
Headquarters Commandant	3420-807
Force Protection Platoon	3420-160

Telephone	
Help Desk	3421-613

LAN	
Help Desk	3420-605

TELEPHONE SECURITY IS EVERYONE'S RESPONSIBILITY. DO NOT DISCUSS CLASSIFIED INFORMATION ON NONSECURE TELEPHONES! OFFICIAL DOD TELEPHONES ARE SUBJECT TO MONITORING AT ALL TIMES FOR COMMUNICATION SECURITY PURPOSES.

CLASSIFICATION

INDEX

EMERGENCY NUMBERS	
GENERAL INSTRUCTIONS	
OPERATING INSTRUCTIONS	
DIALING INSTRUCTIONS	
PRECEDENCE SUBSCRIBERS	
NUMBERING PLAN	
LAN INSTRUCTIONS	
INFORMATION SYSTEMS LISTING	

GENERAL INSTRUCTIONS

TASS allows most subscribers to place local and long distance telephone calls without operator assistance. By using the following instructions telephone service will be quicker and more responsive to your needs. Use the following telephones with digital switching equipment:

TA-1042 Digital Non Secure Voice Terminal (DNVT). This is the ruggedized green push button telephone. The LED will blink and a ring will be sounded when the phone receives a ring. A knob located on the phone will adjust ringer volume. Ensure that the ear-piece is properly reinserted into the body of the phone after the call is completed. DO NOT use the push-to-talk switch on the handset at anytime. This will disrupt your conversation.

KY-68 Digital Secure Voice Terminal (DSVT). This is the ruggedized green push button telephone. Once filled, the KY-68 holds the highest classification because of the COMSEC key loaded inside and must be handled accordingly. After the phone has received its crypto fill it requires no user adjustments other than adjusting the ring volume. ANY OTHER ADJUSTMENTS TO THE REMAINING CONTROLS MAY ZEROIZE THE TELEPHONE RENDERING IT INOPERATIVE. If this occurs notify the TELEPHONE TROUBLE DESK at 411.

SECTEL MMT 1500. This is the Motorola 1500 STU III in that it can be operated from a garrison telephone or the tactical phone system. The MMT can talk unsecured to any type of phone on the tactical system (the MMT can only be connected to the tactical switch digital line termination unit (DLTU) with the DNVT adapter). The MMT can only go secure with another STU-III. The dialing instructions for the MMT are the same as any tactical instrument on the network unless dialing through an IWF.

INTER-WORKING FUNCTION (IWF). This device allows tactical SECTEL MMT 1500 STU-III subscribers to place secure calls to commercial STU-III subscribers. The IWF is programmed as a DNVT within the ULCS network and is direct access service (DAS) to the TTC-42 switch and connected to a single Dial Central Office (DCO) line. Access the IWF by dialing its tactical number from a SECTEL MMT 1500 STU-III within the tactical network, receiving a second dial tone (from DCO) and then dialing the commercial telephone number. Once this connection is made, both subscribers may go secure.

The only way that commercial subscribers are able to go secure with tactical STU-III subscribers is by dialing through the IWF.

OPERATING INSTRUCTIONS

The KY-68 and the TA-1042 may receive and initiate calls with any telephone installed within the TASS. The KY-68 has some unique operation characteristics that are as follows:

- Under the handset of the phone is a 3 position pole type plunger which automatically sets itself in the secure mode when the phone is hung up.
- All calls will be initiated in the secure mode; pick up the handset and dial the required number you desire.
- If the party you are calling does not have a secure voice telephone (KY-68), you will hear a continuous heartbeat sound in the receiver and the NSW (Nonsecure Warning) will flash. Simply pull up on the plunger and your phone will go to the unsecured mode. ***Note: The NSW light will remain until you terminate the call.***
- The KY-68 will automatically reset itself to the secure mode when you hang up.

DSVT's cannot talk secure with STU-III telephones. They are not compatible in the secure mode.

Access Through Defense Switched Network (DSN)

The II MEF TASS will have six DSN trunks available through the AN/TTC-42 switchboard. DSN use by subscribers will be on "A FIRST COME, FIRST SERVED" basis. Precedence subscribers will have the ability to preempt other subscribers when a precedence call is initiated.

DIALING INSTRUCTIONS

- To dial a tactical telephone number from your tactical phone, dial the following:
 - AN/TTC-42 subscribers: Dial 9 and the seven digit extension (9-XXXX-XXX).
- To dial DSN telephone numbers aboard Camp Lejeune from your tactical phone, dial the following:
 - AN/TTC-42 subscribers: Dial 5C (wait for tone)-451-XXXX-C. (XXXX = the four digit DSN number) or dial for the operator at 000.
 - SB-3865 subscribers: Dial 91 (wait for the tone)-5C (wait for the tone)-451-XXXX-C or dial the operator at 000.
- To dial a tactical telephone number from a DSN number or to dial a TASS Operator from a DSN number, take the following steps:
 - Dial the tactical switch operator at one of the following numbers: 6131 or 6174.
 - Give the operator the seven digit number (PRSL-XXX) for the subscriber you wish to reach. **Example: 3469-633.**

Note: TASS subscribers with an assigned higher precedence may start the dialing sequence with the appropriate level precedence.

- If any problem occurs during the dialing process, call the operator by dialing 000 or for telephone trouble calls within your switching network, dial the unit's corresponding telephone trouble desk number.

PRECEDENCE SUBSCRIBERS

The tactical circuit switch (AN/TTC-42) is capable of processing five levels of precedence. The precedence levels in ascending order are—

ROUTINE	(R)
PRIORITY	(P)
IMMEDIATE	(I)
FLASH	(F)
FLASH OVERRIDE	(FO)

The maximum precedence level authorized to a particular terminal is assigned by a classmark. The precedence indicator (P,I,F,FO) is dialed first in any dialing sequence. If no precedence is dialed, the call is processed as routine. Subscribers can initiate calls at a precedence level lower than the maximum authorized. Once a call is established, the originator's precedence level is maintained, regardless of the level authorized to other participating parties. Preemption is employed to calls of higher priority are given preference over lower precedence calls. Initiate the call with the assigned precedence, and the call will be completed on a priority basis. Example: P600, F300, etc.

Note: When a priority is used it will disconnect any subscriber who has lower precedence. PLEASE USE THEM WITH DISCRETION.

WARNING

Remember that the telephone network is NOT SECURE. Do not discuss classified material on any telephone UNLESS YOU ARE USING A KY-68 OR A STU-III TELEPHONE IN THE SECURE MODE. Even calls made within the command post are susceptible to interception. Practice good communications security!

NUMBERING PLAN

The Primary Zone (PR) is the primary identification number that identifies subscribers in the geographic area.

Switch Location (SL) assignments are listed for all commands and organizations within II MEF and east coast units. Spare SL numbers are provided at different echelons and for task organization assignments.

The following PR and SL are assigned to II MEF units participating in the MEF Exercise:

	<u>PR</u>	<u>SL</u>
II MEF CE	34	20
EIGHTH COMM BN	34	21
2D FSSG	35	77
MED BN	35	80
8TH ESB	35	82
2D LSB	35	84
8TH MT BN	35	86
2D MAW/MWCS-28 DET B (CHRY PT)	35	27
2D MAW/MWCS-28 DET A (BOGUE FLD)	35	30
2D MAW (NEW RIVER)	35	32
2D MAW/MWSS-274	35	42
2D MAW/MWSG-27	35	36
2D MAW/MWSS-271	35	40
2D MAW/MASS-1	35	33
2D MAW/MWSS-272	35	41
2D MARDIV	34	69
2D MAR REGT	34	76
6TH MAR REGT	34	77
8TH MAR REGT	34	78
10 MAR REGT	34	79
2D TANK BN	34	88
2D AMPHIBIOUS ASSAULT BN	34	89
2D LAR BN	34	90
2D COMBAT ENG BN	34	91

LAN INSTRUCTIONS

***Disclaimer.** The United States Marine Corps, while recognizing certain commercial products in this directory, does not endorse any of the products listed here. Technology and the marketplace drive the products that are available. The USMC will use the best technology or tool for the job at any given time.*

LAN Overview

II MEF personnel will have access to both the nonsecure internet protocol router network (NIRPNET) and the secure internet protocol router network (SIPRNET) during this exercise. NIRPNET and SIPRNET addresses are located on the information systems listing at the end of this directory.

The overall LAN coordinator for the exercise will be the II MEF Assistant Chief of Staff G-6 Information Systems Management Officer (ISMO), under the cognizance of the II MEF AC/S G-6. The ISMO will be assisted by communications and information systems officers and personnel at each of the Major Subordinate Commands (MSCs). LAN questions and problems should be addressed to the LAN help desk at 3420-605.

II MEF personnel will be using a variety of computers loaded with Microsoft WindowsNT® network and Exchange® software applications during this exercise. WindowsNT® is a multipurpose operating system that integrates a variety of network services. The network services it provides are designed to address requirements in many categories. Windows NT® will be used to connect all of the units within the MEF.

Software Applications

II MEF computers have been installed with several software application packages, which include Microsoft Outlook® and Internet Explorer®, and Message Dissemination System (MDS).

Microsoft Outlook®. This application is used for all electronic mail applications, including calendar and scheduling features, and is accessed via the desktop icon.

Microsoft Outlook® is a desktop information management program that helps the user organize and share information on your desktop and communicate with others. Use Outlook® to manage your messages, appointments, contacts, and tasks, as well as track activities, view and open files, and share information with others.

In Outlook®, information is organized in folders. When the user first starts Outlook®, the Inbox folder opens. Use the Inbox to read and send mail messages, meeting requests, and task requests.

To create a message, point to New on the file menu, and then click **Mail Message**. Enter recipient names in the **To** and **Cc** boxes. Type the subject of the message in the subject box, and then type the message in the text box. When you are ready to send the message, click **Send**.

To quickly go to another part of Outlook®, click a **Shortcut** on the Outlook® Bar to the left of the Inbox. For example, click **Calendar** to open your Calendar folder. The Folder Banner (horizontal bar above the

information viewer) shows the name of the folder you have open. To see a complete list of your folders, click the folder name in the Folder Banner.

The user can use Outlook® as a substitute for Windows Explorer®. To view the files on the hard disk, click **Other** on the Outlook® Bar, and then click **My Computer**, **My Documents**, or **Favorites**.

Outlook® uses views to sort and organize items in a folder. To switch to a different view, click a **view** in the Current View box on the Standard toolbar.

If Microsoft Word® is installed on a computer, use Word® and Outlook® together to create powerful e-mail messages. To turn Word® as your editor on or off, close this message and click **Options** on the Tools menu. On the E-mail tab, select or clear Use Microsoft Word® as the e-mail editor. With Microsoft Word® as your e-mail editor, you can use features such as autocorrect, spell it, bullets and numbering, document map, and highlighter to create your e-mail messages.

The Internet (MS Internet Explorer®). This application is used for all Web access and is accessed via the desktop icon.

The Internet is a collection of computer networks that connects millions of computers across the United States and around the world. Explorer® enables the user to connect to the internet to gain access to vast stores of information on these computers. Double click on the Explorer® icon to access the internet. When a frequently used URL is typed into the Address bar, Explorer® will complete the address. In addition, Explorer® can search through incorrectly typed addresses in order to find a match.

Users can search for web sites using the Explorer® bar. Click on the **search** button on the toolbar: the Explorer® bar appears in the left side of the browser window. Then click on a link to view that page on the right side of the screen while viewing the list of search documents on the left. It is also possible to browse through favorite sites and history folders, channels, or documents.

Users can find information on the web in a variety of ways. When the **search** button is clicked on the toolbar, the Explorer® bar appears to the left of the window. It provides access to a number of search services that offer different kinds of searching capabilities. To find information quickly, type **GO**, **Find**, or **?**, followed by a word or phrase right in the address bar. Explorer® immediately starts a search for the topic. Then, after the user goes to a specific web page, the user can search for the specific text on that page.

Message Dissemination System (MDS). MDS has been installed on II MEF computers for this exercise. The primary function of MDS is the automatic dissemination of Organizational Automatic Digital Network (AUTODIN) messages to various organizational users as MD Users or E-Mail Addressees. This automatic dissemination is based on the Office Code Distribution provided by the Originator of the message in the form of Office Codes assigned to Plain Language Addresses (PLAs) in the heading of a message, and/or Profiles. Messages are made available to MD for processing either electronically via a GateGuard System or on diskette produced by a GateGuard, Personal Computer Message Terminal (PCMT), or other systems using the standard message diskette format.

LAN Security

The internet works by sending information from computer to computer until the information reaches its destination. When information is sent from one point to another, every computer in between has an opportunity to look at what's being sent. This can pose a security problem. Users must understand that classified information must not be sent on unsecured networks. Users should practice good computer security (COMPUSEC) procedures while using the Internet.

II MEF Information Systems Listing

Effective Date: 210800Z October XXXX

Note: The tactical PRSL numbers listed below are based on a draft GBNP switch block proposal dated 26 Aug 98. CISOs are highly encouraged to check with their unit PAL managers before assigning tactical numbers.

Subscriber	Tactical	Commercial	DSN	E-MAIL ADDRESS	
				NIPRNET Domain:	SIPRNET Domain:
II MEF CMD ELEMENT 3420 (TTC-42)				fwd.iimef.usmc. mil	fwd.iimef.usmc. smil.mil
CG	3420-106 (DSVT)		751-9475	cg@domain	cg@domain
CELLULAR		(910) 340-8230			
C/S	3420-103 (DSVT)				
HQ CMDT	3420-807 (DNVT)				
SJA	3420-104 (DNVT)				
PAO	3420-105 (DSVT)				
SGT MAJ	3420-109 (DNVT)				
G-1					
AC/S G-1	3420-114 (DSVT)			g1@domain	g1@domain
PERSONNEL OFFICER	3420-110 (DSVT)				
ADJUTANT	3420-112 (DSVT)				
G-2					
AC/S G-2	3420-203 (DSVT)			g2@domain	g2@domain
G-2 CHIEF	3420-209 (DSVT)				
CIC WATCH OFFICER	3420-225 (DSVT)				
COLLECTIONS OFFICER	3420-211 (DSVT)				
TARGET OFFICER	3420-245 (DSVT)				
RAD BN	3420-201 (DSVT)				
CI	3420-211 (DSVT)				
METOC	3420-240 (DSVT)				
SARC	3420-242 (DSVT)				
RECON OPS CENTER	3420-244 (DSVT)				
G-3					
AC/S G-3	3420-300 (DSVT)			g3@domain	g3@domain
G-3 CHIEF	3420-303 (DSVT)				
COMBAT OPERATIONS CENTER (COC)					
SENIOR WATCH OFFICER	3420-300 (DSVT)				
FUTURE OPS OFFICER	3420-327 (DSVT)				
AIR OPS OFFICER	3420-308 (DSVT)				

Subscriber	Tactical	Commercial	DSN	E-MAIL ADDRESS	
				NIPRNET Domain:	SIPRNET Domain:
CSS OPS OFFICER	3420-405 (DSVT)				
FFCC OFFICER	3420-340 (DSVT)				
FIRES	3420-340 (DSVT)				
TARGETING	3420-319 (DSVT)				
EW PLANS OFFICER	3420-225 (DSVT)				
CIVIL AFFAIRS	3420-105 (DSVT)				
G-4					
AC/S G-4	3420-402 (DSVT)			g4@domain	g4@domain
G-4 CHIEF	3420-402 (DSVT)				
G-4 OPERATIONS	3420-403 (DSVT)				
EMBARK	3420-404 (DSVT)				
ENGINEER OFFICER	3420-405 (DSVT)				
MEF SURGEON	3420-430 (DSVT)				
G-5					
AC/S G-5	3420-500 (DSVT)			g5@domain	g5@domain
DEP G-5	3420-501 (DSVT)				
G-5 CHIEF	3420-505 (DSVT)				
G-6					
AC/S G-6	3420-600 (DSVT)			g6@domain	g6@domain
G-6 OPS OFFICER	3420-601 (DSVT)				
G-6 OPS CHIEF	3420-602 (DSVT)				
G-6 DATA OFFICER	3420-603 (DSVT)				
G-6 COMM CHIEF	3420-603 (DSVT)				
LAN/WAN TROUBLE DESK	3420-605 (DNVT)				
MISCELLANEOUS					
AID STATION	3420-155 (DNVT)				
FORCE PROTECTION	3420-160 (DNVT)				
8TH COMM BN 3421 (SB-3865)					
CO	3421-806 (DSVT)				
XO	3421-807 (DSVT)				
SGT MAJ	3421-808 (DNVT)				
OPS OFFICER	3421-830 (DSVT)				
OPS CHIEF	3421-931 (DSVT)				
PERSONNEL OFFICER	3421-801 (DNVT)				
BAS	3421-867 (DNVT)				
BN OOD	3421-802 (DNVT)				
SYSCON	3421-613 (DSVT)			syscon@domain	syscon@domain
TECHON	3421-623 (DSVT)			techcon@domain	techcon@domain
DATA COM	3421-633 (DSVT)			datacom@domain	datacom@domain

Subscriber	Tactical	Commercial	DSN	E-MAIL ADDRESS	
				NIPRNET Domain:	SIPRNET Domain:
2D MARINE DIVISION 3469 (TTC-42)				fwd.2dmardiv.iimef. usmc.mil	fwd.2dmardiv.iimef. usmc.smil.mil
CG	3469-106 (DSVT)			cg@domain	cg@domain
G-1	3469-114 (DSVT)			g1@domain	g1@domain
G-2	3469-200 (DSVT)			g2@domain	g2@domain
G-3	3469-300 (DSVT)			g2@domain	g3@domain
G-4	3469-400 (DSVT)			g-4@domain	g4@domain
CELLULAR		(910) 340-8235			
TCO DIAL-IN	3469-675 (DNVT)				
G-6	3469-600 (DSVT)			g6@domain	g6@domain
CELLULAR		(910) 340-1014			
DIVISION COMM COMPANY					
CO COMM CO	3469-610 (DSVT)				
TECHCON	3469-113 (DSVT)				
OPS OFFICER	3469-149 (DSVT)				
SYSCON (STU-III)	3469-669 (DSVT)		751-9265		
SIPRNET to MEF	3469-330 (DSVT)				
TSC-93 (GMF)		(910) 451-9271			
DASC (STU-III)		(910) 451-9272			
LONG LOCAL - MEF	3469-701 (DNVT)				
LONG LOCAL - WING	3469-702 (DNVT)				
TTC-42 (SWBD)			751-9470		
2ND MAR REGT 3476 (SB-3865)					
CO	3476-106 (DSVT)				
S-1	3476-114 (DNVT)				
S-2	3476-200 (DSVT)		751-1014		
S-3 (STU-III)	3476-300 (DSVT)		751-5263		
S-4	3476-400 (DNVT)				
S-6	3476-600 (DSVT)				
6TH MAR REGT 3477 (SB-3865)					
CO	3477-675 (DSVT)				
S-1	3477-200 (DNVT)				
S-2	3477-300 (DSVT)				
S-3	3477-662 (DSVT)				
S-4 (FAX)	3477-400 (DNVT)		751-3977		
S-6 (STU-III)	3477-600 (DSVT)		751-2822		

Subscriber	Tactical	Commercial	DSN	E-MAIL ADDRESS	
				NIPRNET Domain:	SIPRNET Domain:
8TH MAR REGT 3478 (SB-3865)					
CO	3478-106 (DSVT)				
S-1	3478-114 (DNVT)				
S-2	3478-200 (DSVT)				
S-3	3478-300 (DSVT)				
S-4	3478-400 (DNVT)				
S-6 (STU-III)	3478-600 (DSVT)		751-2551		
10TH MAR REGT 3479 (SB-3865)					
CO	3479-106 (DSVT)				
S-2	3479-200 (DNVT)				
S-3	3479-300 (DSVT)				
S-4	3479-400 (DNVT)				
S-6	3479-600 (DSVT)				
2D TANK BN 3488 (SB-3865)					
CO	3488-106 (DSVT)				
S-3	3488-300 (DSVT)				
2D AMPH ASSAULT BN 3489 (SB-3865)					
CO	3489-106 (DSVT)				
S-3	3489-300 (DSVT)				
2D LAR BN 3490 (SB-3865)					
CO	3490-106 (DSVT)				
S-3	3490-300 (DSVT)				
2D COMBAT ENG BN 3491 (SB-3865)					
CO	3491-106 (DSVT)				
S-3	3491-300 (DSVT)				
2D FFSG 3577 (TTC-42)				fwd.2dfssg.iimef. usmc.mil	fwd.2dfssg.iimef. usmc.smil.mil
CG (STU-III)	3577-106 (DSVT)			cg@domain	cg@domain
G-1	3577-114 (DSVT)			g1@domain	g1@domain
G-2	3577-200 (DSVT)			g2@domain	g2@domain
G-3	3577-300 (DSVT)			g3@domain	g3@domain
G-4	3577-440 (DSVT)			g4@domain	g4@domain
G-6	3577-606 (DSVT)			g6@domain	g6@domain

Subscriber	Tactical	Commercial	DSN	E-MAIL ADDRESS	
				NIPRNET Domain:	SIPRNET Domain:
H&S BN					
CO	3577-706 (DSVT)				
S-3	3577-703 (DSVT)				
S-4	3577-704 (DNVT)				
FSSG COMM CO					
CO	3577-610 (DSVT)				
OPSO	3577-149 (DSVT)				
SYSCON	3577-633 (DSVT)				
COMMERCIAL (STU-III)		(910) 451-9609			
TECHCON	3577-669 (DSVT)				
SUPPLY	3577-720 (DNVT)				
MAINT	3577-779 (DNVT)				
COMMERCIAL (STU-III)		(910) 451-9610			
MD BN 3580 (SB-3865)					
CO	3580-706 (DSVT)				
S-3	3580-703 (DSVT)				
S-4	3580-704 (DNVT)				
S-6	3580-600 (DSVT)				
DENTAL BN	3580-604 (DNVT)				
ENG BN 3582 (SB-3865)					
CO	3582-706 (DSVT)				
S-3	3582-703 (DSVT)				
S-4	3582-704 (DNVT)				
S-6	3582-600 (DSVT)				
LSB 3584 (SB-3865)					
CO	3584-706 (DSVT)				
S-3	3584-703 (DSVT)				
S-4	3584-704 (DNVT)				
S-6	3584-600 (DSVT)				
MT BN 3586 (SB-3865)					
CO	3586-706 (DSVT)				
S-3	3586-703 (DSVT)				
S-4	3586-704 (DNVT)				
S-6	3586-600 (DSVT)				

Subscriber	Tactical	Commercial	DSN	E-MAIL ADDRESS	
				NIPRNET Domain:	SIPRNET Domain:
2D MAW CHERRY POINT 3527 (TTC-42)				fwd.2dmaw.iimef. usmc.mil	fwd.2dmaw.iimef. usmc.smil.mil
CG	3527-106 (DSVT)			cg@domain	cg@domain
G-1	3527-114 (DSVT)			g1@domain	g1@domain
G-2	3527-200 (DSVT)			g2@domain	g2@domain
G-3	3527-300 (DSVT)			g3@domain	g3@domain
G-4	3527-400 (DSVT)			g4@domain	g4@domain
G-6	3527-675 (DSVT)			g6@domain	g6@domain
TACC "DET B" CHERRY POINT					
SYSICON OFFICER	3527-113 (DSVT)				
TECHCON	3527-150 (DSVT)				
TSC-85	3527-185 (DNVT)				
TSC-120	3527-120 (DNVT)				
TSC-96	3527-196 (DNVT)				
TRC-170 (MEF)	3527-170 (DNVT)				
Long Local - MEF	3527-613 (DNVT)				
MCWS 28 CO	3527-106 (DSVT)				
MCWS 28 S-3	3527-103 (DSVT)				
MCWS 28 S-4	3527-104 (DSVT)				
MCWS 28 Maint	3527-115 (DNVT)				
DET B OFFICE	3527-206 (DNVT)				
DATA COMM	3527-230 (DSVT)				
COMM CENTER	3527-111 (DSVT)				
MSC-63	3527-211 (DNVT)				
MTACS 28					
SAC	3527-333 (DSVT)				
CTAPS SYS ADMIN	3527-380 (DNVT)				
SWO/SAC	3527-334 (DNVT)				
DCN	3527-382 (DSVT)				
ICO	3527-393 (DSVT)				
TACC	3527-381 (DSVT)				
2D MAW BOGUE FIELD DET "A" 3530 (TTC-42)					
SYSICON	3530-113 (DSVT)				
TTC-42 VAN	3530-555 (DNVT)				
TECHON	3530-150 (DSVT)				
CO	3530-106 (DSVT)				
RADIO	3530-132 (DNVT)				
WIRE	3530-131 (DNVT)				

Subscriber	Tactical	Commercial	DSN	E-MAIL ADDRESS	
				NIPRNET Domain:	SIPRNET Domain:
DATA COMM	3530-129 (DSVT)				
COMM CTR	3530-111 (DSVT)				
MAINT	3530-115 (DNVT)				
MACS-6 ATC SITE					
ATC COMMON	3530-350 (DNVT)				
FACILITY WATCH O	3530-351 (DSVT)				
RADAR SUPERV	3530-352 (DNVT)				
MACS-6 EW/C SITE					
SAD	3527-330 (DSVT)				
SID	3527-332 (DSVT)				
TECHCON	3527-313 (DSVT)				
SYSCON	3527-310 (DSVT)				
NEW RIVER DET "A" 3532 (SB-3865)					
SYSCON	3532-113 (DSVT)				
SYSCON (SWO)	3532-213 (DSVT)				
TTC-42 VAN	3532-150 (DNVT)				
TECHON	3532-150 (DSVT)				
CO	3532-106 (DSVT)				
MASS-1 SUBSCRIBERS 3533 (SB-3865)					
SAC	3533-101 (DSVT)				
SYSCON	3533-102 (DSVT)				
SEC WAN	3533-103 (DSVT)				
COMM USER	3533-104 (DNVT)				
MAG-26 NEW RIVER 3535 (SB-3865)					
CO	3535-106 (DSVT)				
S-1	3535-114 (DSVT)				
S-3	3535-300 (DSVT)				
S-4	3535-400 (DSVT)				
S-6	3535-600 (DSVT)				
HMLA-167					
CO	3535-806 (DSVT)				
S-3	3535-330 (DSVT)				
MWSG 27 3536 (SB-3865)					
CO	3536-806 (DSVT)				
S-3	3536-803 (DSVT)				
S-6	3536-800 (DSVT)				

Subscriber	Tactical	Commercial	DSN	E-MAIL ADDRESS	
				NIPRNET Domain:	SIPRNET Domain:
S-6 CHIEF	3536-801 (DNVT)				
SYSCON	3536-802 (DSVT)				
TECHCON	3536-833 (DSVT)				
DATA	3536-804 (DSVT)				
WXO	3536-805 (DNVT)				
MWSS 271 3540 (SB-3865)					
CO	3540-506 (DSVT)				
S-3	3540-503 (DSVT)				
S-6	3540-500 (DSVT)				
SYSCON	3540-501 (DNVT)				
TECHON	3540-502 (DNVT)				
WXO	3540-505 (DNVT)				
MWSS 272 3541 (SB-3865)					
CO	3541-506 (DSVT)				
S-3	3541-503 (DSVT)				
S-6	3541-500 (DSVT)				
SYSCON	3541-501 (DNVT)				
TECHON	3541-502 (DNVT)				
WXO	3541-505 (DNVT)				
MWSS 274 3542 (SB-3865)					
CO	3542-306 (DSVT)				
S-3	3542-303 (DSVT)				
S-6	3542-300 (DSVT)				
SYSCON	3542-301 (DNVT)				
TECHON	3542-302 (DNVT)				
WXO	3542-305 (DNVT)				

Appendix F

CIS Planning Checklist

The purpose of this checklist is to guide CIS planning for joint operations. This checklist is derived from Joint Pub 6-02, *Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems*. This checklist is not all-inclusive. Questions should be revisited as CIS planners adapt to the changing operational situation. The checklist provides a framework for supporting CIS planning for each phase of an operation, focusing CIS planners on the mission and how the commander intends to accomplish it. CIS planners should also be familiar with relevant joint and naval TTP and have access to pertinent publications and technical manuals as well as CIS support organizations, including those listed at appendix P.

Reference Material

- Existing OPLANs and OPORDs
- Commander's planning guidance, estimate, intent, and concept of operations
- Area studies
- Unit SOPs
- Joint Pub 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support for Joint Operations*
- Joint Pub 6-02, *Joint Doctrine for Employment of Operational/Tactical Command, Control, and Computer Systems*
- Joint Pub 6-02.1, *Joint Connectivity Handbook*
- CJCSM 6230.03, *Communications-Electronics Operations Instructions—Signal Operations Instruction*
- CJCSM 6231.01–6231.07A series, *Manual for Employing Joint Tactical Communications*
- DISA Contingency Plan 10-95
- *Joint Communications Support Element Planning Guide*
- Lessons-learned databases from previous operations and exercises
- TPFDD and time-phased force deployment list

Planning Considerations

General

- What is the MAGTF or unit mission?
- What is the geographic operational area?
- What are the commander's intent, concept of operations, planning guidance, and CCIRs?
- What are the commander's communications and information systems requirements?
- What are the JTF, naval expeditionary force, MAGTF, and supporting elements' task organizations? What are the command relationships?
- How will the forces deploy (means of transportation), and what is the deployment timeline?
- Are there any transport and/or lift restrictions (availability of assets, departure and arrival locations)?
- Are there any satellite landing rights?
- When are the operations planning meetings scheduled? How will CIS planning meetings fit into this schedule? Has DISA been involved regarding coordination of technical requirements?
- Are there any planning constraints?
- Are there any special CIS requirements? Who has them?
- What national space-based assets are required and/or available to support the operation? Has a U.S. Space Command Joint Space Support Team been contacted?
- What communications capabilities are available to the MAGTF: SHF and/or UHF commercial satellite, DSCS, and FLTSATCOM;

military strategic and tactical relay system (Milstar) satellite terminals; JWICS and Milstar; HF, VHF, and UHF radio; tropospheric and line-of-sight microwave systems; local area, switched backbone, and router networks; DMS; DISN; and personal communications systems?

- What frequencies are available for the MAGTF in the operations area?
- What are the general INFOSEC requirements? Who will draft the callout message?
- Who is the potential adversary? What are their capabilities to conduct offensive information warfare (IW)? Does a joint force plan exist to counter the threat?
- What are the releasability requirements for multinational operations?

Subordinate Units

- Where will their C2 nodes be located?
- What are their communications requirements (identify by function, C2 node/agency, and overall unit priority)?
- What are their communications capabilities (identify by function, command and control node/agency, and overall unit priority)?
- What type of communications systems do they have (power, frequency bands, interoperable and compatible with other subordinate components' equipment, mobility)?
- Who is the unit CIS officer (G-6 or S-6) staff point of contact for planning and technical management and direction?
- Are there any special CIS requirements resulting from the mission and the commander's estimate, intent, and concept of operations?
- Are subordinate and supporting CIS plans consistent with the supported commander's CIS plan?

Supporting Units

- What is the mission of the supporting units and/or activities (this includes other Services, agencies, allies, and coalitions)?
- What are their communications capabilities?

- What information does the supported MAGTF or unit need from the supporting units and/or activities (intelligence, weather, imagery, mapping, deployment), and how will it be accessed?

Nonorganic Support

DISA

- Does the operational area have a DISA Regional Control Center or field office?
- Who is the DISA point of contact?
- What is the DISN infrastructure in the operational area?
- Are sufficient gateways available? What are the interface requirements to access the gateways? Is the equipment available?
- Is the Telecommunications Service Provisioning and/or National Security Emergency Preparedness authority provided and current?
- What are the anticipated DSCS and commercial satellite requirements?
- Has modeling of space networks been initiated by DISA?

Commercial Networks

- Are commercial networks available for use? Who can approve access to them? Are funds available? Has DISA been contacted to ensure required lead times for normal allocations? (1) Satellite (2) Data (3) Voice?
- What special interfaces are required to access the commercial network, and where are the access points?
- What are the locations and types of switches in the commercial network? What are their technical parameters?
- Where are the locations and types of systems providing the backbone transmission network?
- What type of power is used—voltage, current, commercial grid, or generator?
- Does the operational area have a cellular network? What are the transmission media, frequency band, and interface requirements? What are the system standards? Is the system available for use?

Chairman of the Joint Chiefs of Staff (CJCS)-Controlled Assets

- What CJCS-controlled assets are available?
- What capabilities are available?
- Will JCSE support be required in the operational area, or will other defense and commercial assets be sufficient?
- Will JCSE support be needed for en route communications?
- Has a Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6110.01, *CJCS-Controlled Tactical Communications Assets*, support request for CJCS-controlled C4 systems assets been submitted?
- What are the JCSE's logistics support and electrical power requirements?
- What are the JCSE airlift considerations, allocations, and/or priority?

Other Support

- Is support needed from specialized communications units?
- Who are the points of contact, and what are the request procedures?
- What are the unit's communications capabilities and limitations?

Planning Activities**General Planning**

- What nodes will provide entry into the global C⁴ systems network, and where will they be located?
- What transmission media will be used to connect the nodes?
- What types of CIS equipment will be located at each node (equipment strings, interoperability of the equipment)?
- What are the frequency requirements for each node? How will the frequencies be allotted (joint, multinational, components, the MAGTF, and MSCs)? Are there potential frequency conflicts?

- What are the call signs and/or words for each node?
- What units will provide, install, operate, and maintain the equipment for each node?
- What lift assets are available to deploy these units? When will the units deploy and activate the nodes or network?
- Is the deployment schedule of CIS assets consistent with the phases of the plan? Will it permit the provision of CIS support when and where needed?
- What is the phased buildup of CIS in the operational area?
- Has CIS scheduling information been added to the TPFDD and/or time-phased force deployment list?
- Have the commander and principal staff officers affected been informed of potential CIS shortfalls and recommended solutions?
- How will keying material be managed (ordering, generation, storing, distribution, transfer, and destruction)? What are the procedures for handling compromises? Is a COMSEC logistics management activity needed in the operations area? What access will allies have to U.S. COMSEC?
- Are network and node diagrams available?
- Have special communications requirements been addressed (MPF, shipboard, SAR, en route communications, and embarkation and debarkation connectivity)?
- Have SCI communications requirements been identified and satisfied?
- How will the joint, component, supporting forces, and MAGTF networks interface with nonorganic networks (DISN, commercial, and JCSE)?
- When and where will the joint, Marine Forces, or MAGTF communications control centers be established?
- Are the subordinate elements/units and supporting CIS plans consistent with the MAGTF CIS plan?

Detailed Planning**Circuit Switches**

- Does a circuit switch network diagram exist that shows information about the switch and circuit switch network connectivity (switch type, area code, trunk groups, and capacity)?
- How does the switch route calls: flood, deterministic, or circuit switch routing task execution plan?
- Where do circuit switches need to be located? How will they be connected?
- What special features or restrictions will be imposed on subscribers? Who will authorize and enforce these restrictions?
- Where are the DSN interfaces? Are precedences authorized? By whom?
- How will subscriber assistance be handled?
- Where is the greatest anticipated traffic load: for GENSER? for SCI? Does sufficient capacity exist to handle these?
- What types of status reports are required, and when will they be submitted?
- How will traffic metering and network loading be measured, modeled, and managed?
- Who will publish telephone directories, and how will they be distributed?

Data Networking

- What are the anticipated MAGTF or unit data requirements?
- Has automation been planned and/or engineered into the network (x.25, IEEE 802.3, TCP/IP)?
- What and/or where are the network identifications and gateways?
- Will data of various classifications “ride” a secure tactical backbone? How will traffic of various classifications be controlled and managed? Are multilevel information systems security initiative devices needed, and are resources available?
- What is the data network architecture?
- Who are the data network managers?
- What are the NIPRNET, SIPRNET, and JWICS connectivity requirements?

- What STEP sites will be used? Has a gateway access request been submitted in accordance with DISA contingency and/or exercise plans?
- What is the addressing scheme?
- Where do the IP addresses come from?
- Will the IP addresses have to be changed when elements of the MAGTF go ashore?
- What is the scheme for sorting out router loops?

Message Switches

- Where are the message switches required?
- What is the trunking plan?
- What is the network connectivity of all message switches?
- Have routing indicators been developed and routing tables established?
- Is this an R and/or Y network?
- Has a plain language address directory been created?
- How will special category traffic be handled? Who will be authorized to have access?
- What are the intranodal and internodal terminals?
- What types of status reports are required, and when will they be submitted?
- What AUTODIN switching centers are connected to the message switch?
- Who is the automated message processing system security officer?
- Who will act as the AUTODIN controller?

Transmission Systems

- Are the circuit requirements, routing, channelization, and other parameters that were identified in high-level planning valid? Have satellite access requests been submitted? Have frequency requests been approved and published?
- What are the characteristics and connectivity of multiplexers in the network? Are they compatible?

- What are the timing requirements for the network components? How will timing be accomplished?
- What types of status reports are required, and when will they be submitted?

Technical Management and Direction

Joint, Marine Forces, and/or MAGTF Communications Control Centers

- What are the operational procedures for the control centers?
- Where are the joint, Marine Forces, and/or MAGTF control centers located?
- How will the control centers be manned?
- What reports will be required, how often will they be required, and when will they be submitted?
- How will network reconfiguration be accomplished?
- Who are the points of contact at the subordinate control centers?
- Who will submit the telecommunications service request (TSR) and telecommunications service order (TSO)? Have TSRs/TSOs for SCI communications requirements been incorporated?
- Who will coordinate changes to connectivity with the DISN? With the commercial networks?
- What kind of statistics will be kept? Who will analyze them? What will be done with them?
- How will changes caused by the evolving tactical situation be handled?
- Can the JCCC direct changes within MAGTF networks to optimize C⁴ systems within the joint operations area?
- Where is the boundary between technical direction and operational direction?
- How will frequency deconfliction be managed? How can potential conflicts be anticipated?

- Who will control frequency spares and authorize their use?
- Who manages the allocated satellite bandwidth used by the geographic joint forces?

JCSE

- Is JCSE support required?
- Who is the JCSE point of contact?
- How is support requested?
- How will JCSE participate in the technical management process?
- Are there any special reporting requirements for systems provided by the JCSE?

Spectrum Management

- What are the provisions and procedures for frequency planning and use for opposed and/or unopposed entry operations into an operational area?
- What frequency allotments and assignments are available for the operational area?
- Can the allotted and assigned frequencies support the equipment deployed to the operational area (communications, LANs and/or WANs, sensors, surveillance radars, GPS, and airspace control radars)?
- Will the frequencies work (propagation and topographic analyses)?
- Does the allocation and assignment of frequencies to subordinate commands contribute to mission accomplishment?
- What are the enemy capabilities to intercept, radio direction find, jam, or otherwise exploit or degrade MAGTF allotted and assigned frequencies? Does a joint and MAGTF plan exist to counter the threat?
- Will the JCCC resolve electromagnetic interference issues? Will Joint Spectrum Center support be required to resolve interference issues?
- Who will issue the Joint Restricted Frequency List?

- Are sufficient spare frequencies available?
- What EMCON measures will be applied?
- Will the MAGTF implement an electronic deception plan? Are sufficient frequencies available to support this plan?

Security

- Will the cryptographic equipment interoperate?
- What are the keying material requirements?
- Does a key management plan exist?
- How will cryptographic compromises be detected and corrected?
- What INFOSEC measures will be employed on the LANs and WANs in the operational area?
- How will access to the various networks be controlled (electronic and physical)?
- Have COMSEC and INFOSEC emergency destruction procedures been established?
- What is the logistics plan for the cryptographic equipment?
- Are equipment and keymat sufficient to support planned and unplanned operations?
- Have key change times been established and promulgated?
- Have provisions been made for over-the-air re-keying where applicable?
- Is an intertheater communications plan available? Is it needed?
- What will we transition to and when?
- What is the IW threat?
- Are virus-detection software applications installed and operational? Are passwords issued and in use? Has a contingency plan been developed to guide recovery actions should data be modified or destroyed by unauthorized intrusions?
- Do remotely accessed computer systems possess features to identify users and substantiate their identification before allowing information to be processed?

Appendix G

Unit Planning Checklist

The following checklist is provided to assist CIS planners in conducting operational planning. It is oriented toward detailed unit planning from a CIS perspective. This checklist is based on the 6-Step Marine Corps Planning Process (MCP) published in MCWP 5-1 (draft). Rather than reiterate the specific subcomponents of the 6-Step MCP, the reader should refer to MCWP 5-1 and comparatively analyze thought processes which may assist in the design of the overall CIS architecture(s) which support one or more courses of action (COAs).

The recommendations which follow may not be complete, depending on the level of planning, the time allocated for planning, and most importantly, the commander's intent. As with any collaborative planning, the MCP may not always appear sequential (e.g., 1, 2...6) when actually being executed. With these thoughts in mind, the considerations provided below apply to each step, but are not necessarily limited to any specific step. This is because the operational planning team (OPT) must remain focused on the commander's intent—and supporting it—throughout all levels of planning.

Step 1, Mission Analysis

During this step, it is essential that the CIS planner develop a thorough understanding of the mission and the commander's intent, as well as the situation. Included in this step are—

- Commander's initial orientation.
- Staff analysis—the CIS planner may begin to consider some of the following:
 - Connectivity.
 - JTF HQ? MARFOR HQ? What is the MAGTF composition?
 - Links to MSCs; again, MAGTF composition?
 - Strategic high-capacity links—are these required?
 - What special capabilities may be required to support special circuits?
 - Is bandwidth adequate?
 - MUX, SCR, what is the operational state—transitional (mobile) or consolidated (more static), and how may we support this?
 - Interoperability—like all CIS planning the key planning considerations (flexibility, survivability, etc.); the CISO should consult the CJCSM 6231.07A to determine if equipages involved in the operation are interoperable.
- Coordination—as soon as feasible, plan and conduct an initial planning conference for CIS personnel (to include adjacent and subordinate unit G-6/S-6s) in order to begin effective, concurrent planning. Coordinate all issues as they can be developed. Determine mid-term planning conference as applicable to update all personnel involved in the planning with the latest revisions and commander's intent.
- Intelligence preparation of the battlespace (IPB). As with all members of the staff, IPB should be constant throughout the planning

process. Some initial considerations include—

- Location/distances with respect to the enemy; what terrain studies are available?
 - Begin analysis of the topography and environment in which CIS systems must operate. Consider also time of year (TNAPS + databases can begin to be built, notional at this point, and/or SPEED can be used to assist in this initial analysis of the area of operation).
 - Electronic emissions, communications security (COMSEC), computer security (COMPUSEC) and physical security issues must be formulated from the initial planning. What are enemy and friendly electronic warfare (EW) capabilities?
 - Ensure a thorough understanding of the enemy's location and situation. Possible node and retransmission sites must be considered in light of the enemy situation.
- Warning order.

Step 2, COA Development

The CIS planner should consider all factors that affect the exercise of C2. These factors include mission, allocated forces, supporting communications units and equipment employment sites, and joint/MAGTF user requirements. Finally, develop alternative approaches to satisfy C2 requirements.

- Determine desired end state; some specific CIS considerations may include—
 - Asset availability; what units are available to support the current COA?
 - Personnel availability; what personnel can best provide mission support to the COA?
 - Tempo of the operation; in addition to mobility factors, how do all of the battlespace functions factor in which must be supported by CIS systems?

- Synchronization of C2 with maneuver and all warfighting functions mobility of the CIS assets and personnel?
- Provision for link or circuit activation—speed of support vs. reliability of the link or circuit must be weighed; priority ALWAYS rests with the commander.
- Force protection; how do CIS units and personnel support force protection?
- Logistics considerations; provision of support must be matched by effective consideration of the logistics plan.
- IPB results; IPB is continuous, and the enemy situation as it develops must be in the CIS planner's mind.
- Develop measures of effectiveness (MOEs).
- Develop COAs to achieve end state.
- Present COA brief.
- Obtain approval of COAs for further analysis.

Step 3, COA Analysis

The CIS planner must analyze all alternatives to determine advantages and limitations of each.

- Commander provides guidance.
- Staff wargames each COA.
- Staff briefs each COA.
- Wargame results.
- Staff estimates of supportability.
 - Feasibility of all alternatives to support the COA?
 - Adequacy of all means to support the COA?
 - Acceptability of mediums and capacities (links, circuits, etc.) to the commander?
 - Supportability of the CIS plan for the COA; does it best enable the commander to exercise C2? What are the commander's critical information requirements (CCIRs),

and how may each link/circuit provide them?

- Assumptions with regard to availability of assets and personnel; identify and reconcile all of these with the commander.
- Limitations; the estimate of supportability should identify for the commander and staff what these may be.
- Constraints/restraints; how do they affect the design and implementation of the CIS plan?

Step 4, COA Comparison and Decision

Selecting the best COA relies heavily on the development of the COA by staff elements; it is at this point that the CIS planner assists the commander and staff in COA comparison by recommending the best option.

- Commander evaluates and compares COAs.
- Commander decides on the COA to be used.
- New warning order issued.
 - Commander's concept of operation.
 - Updated commander's intent.
 - Complete description of the chosen COA.
- Supporting concepts; the CIS planner must begin immediately to resolve any shortfalls anticipated. At this point, the limitations which have already been identified by the CIS planner must be reduced or overcome in order to support the commander's ability to exercise C2.
- Task organization.
- Refined CCIRs.
- Staff estimates.
- Coordination—the CIS planner should ensure that final coordination with all respective G-6s/S-6s (or designated representatives) is completed prior to orders development. During the planning

phase, coordination of a final planning conference and a technical control conference will enable key coordination efforts to take place, and a more detailed plan for support can be prepared by all supporting units/agencies.

Step 5, Orders Development

Prepare the Annex K, refine the plan continuously, and continue liaison with the staff and the commander. In this step, the staff will refine the selected COA into an OPORD together with supporting documentation. Much of the required information will have already been developed in the previous steps of the planning process. The checklists below identify specific areas to be addressed in the OPORD.

The first list should be checked as soon as you know your mission, while the second contains items to be addressed after receipt of a warning order. Many of these areas will need to be addressed several times throughout the planning and during execution. Bear in mind that planning for an operation/exercise is different from planning for a contingency. The checklists on the following pages are to help guide you.

Items to be Initiated Well in Advance of Warning Order Receipt

*These items require continuous action before and during the operation.

Communications

- Review senior HQ operation plan/letter of instruction.
- Identify command relationships and related connectivity requirements (both GENSER and SCI).*
- Request maps of area of operation.
- Determine equipment requirements.*
- Conduct map, weather, terrain analysis.*
- Conduct C2 threat assessment. (See app. K.)

- Conduct site or map reconnaissance and ID possible CP locations.*
- Conduct SPEED/sight analysis tools/Joint Spectrum Center studies.
- Request frequencies/net IDs/call signs.
- Submit UHF satellite request (CUDIXS).
- Submit SHF/GMF satellite access request.
- Identify AUTODIN requirements.
- Submit telecommunications service requests (both GENSER and SCI).
- Recommend/coordinate w/S-3 on CP layout.
- Identify retransmission/relay/remote locations.*
- Determine security requirements for communications assets (both GENSER and SCI).
- Coordinate messenger communications operations and procedures with the unit G-1/S-1.
- Review SYSCON procedures.
- Identify communications reporting procedures.
- Prepare and distribute radio guard chart.
- Prepare and distribute IP address chart.
- Prepare circuit switch traffic diagram.
- Provide senior HQ with CEOI/automated CEOI/telephone directory.
- Conduct ship visit (see app. C) as soon as possible.
- Present predeployment briefing to staff/subordinates.
- Publish communications-related safety reminders.
- Prepare for special operations if required.
- Conduct predeployment training.
- Assess environmental impact on communications.
- Review appropriate publications.
- Ensure that subordinate units understand communications guard shift procedures.
- Prepare/submit communications guard shift in accordance with NTP 4, *Naval Telecommunications Procedures—Fleet Communications*.

Maintenance

- Verify an equipment repair order matrix.
- Determine repair parts requirements (preexpended bin, class IX block, stocks).
- Review/establish maintenance procedures.
- Check force activity designator status.
- Determine technicians required.
- Update the equipment repair order priorities on mission-essential equipment (Marine Corps Bulletin 3000).
- Update priorities on modifications and calibrations.
- Determine availability/need for mobile maintenance teams.
- Prepare necessary publications for embarkation.
- Conduct liaison visits with support agencies.
- Update temporary loan paperwork.
- Determine status of type I, II, and III items.
- Determine MPF asset availability.
- Prepare tools/equipment (test, maintenance, and diagnostic equipment).
- Conduct limited technical inspections.
- Update preventive maintenance actions.
- Determine availability of maintenance facilities.

CMS/Classified Materials Control Center/Security

- Establish list of authorized users.
- Determine keying material requirements.
- Acknowledge satellite access authorization.
- Determine CMS start and changeover times.
- Determine requirement for safes.
- Determine requirement for cables.
- Issue security reminder to all users/staff (two-person integrity).
- Prepare input for C2 protection and deception plan.
- Establish message handling procedures.

- Determine hardware requirements.

Items to be Initiated After Receipt of a Warning Order

Communications

- Issue fragmentary/warning order to subordinate units and issue initial CIS guidance to supported principal staff officers.
- Assemble staff to begin detailed planning.
- Submit equipment augmentation request.
- Weatherproof equipment.

Maintenance

- Conduct operational checks.

CMS.

- Issue CMS callout message.
- Ensure that CMS equipment is distributed.

Administration

Personnel Equipment Requirements

- Helmet.
- Flak jacket.
- H-harness.
- Cartridge belt.
- Two canteens with covers.
- Two magazine pouches.
- Six M-16 pouches.
- Weapon (with cleaning gear).
- Chemical protective gear.
- Gas mask.
- E-tool.
- ALICE pack (with frame).
- Flashlight (red lens).
- Bayonet/K-bar.
- Ear plugs.

- Shelter half (with five pins, three poles, and guy line).
- ISO mat.
- Waterproof bag.
- Sleeping bag.
- Poncho and poncho liner.

Uniform Requirements

- Cammies.
- Cammie cover.
- Physical training gear (green/green, gray/gray, running shoes, white socks).
- Field jacket with liner.
- Watch cap.
- Gloves with inserts.
- Rank insignia.
- Combat boots.
- Boot bands.
- Web belt with buckle.
- Cold-weather underwear (top and bottom).
- Wet-weather top.
- Wet-weather bottom.
- Skivvie bottoms.
- T-shirt.
- Socks.
- Civilian clothes.
- Towel (green).
- Washcloth (green).
- Shaving kit.
- Foot powder.
- Boot polish and brush.
- Sewing kit.

Personnel Administrative Requirements

- Determine personnel requirements.
- Ensure that security clearances are complete.
- Identify advance, main, and rear parties.
- Make advance party assignments.

- Submit request for personnel augmentation.
- Determine billeting requirements.
- Duplicate records (service record book, health, dental,).
- Ensure that visas/passports/drivers licenses (Status-of-Forces Agreement) are current.
- Ensure that basic clothing is servicable/marked.
- Ensure that direct deposit is established.
- Ensure that powers of attorney are completed.
- Ensure that wills are completed/updated.
- Check dental (class I or II) status.
- Check dependent care arrangements.
- Obtain key volunteers phone list.
- Ensure that mail (forwarding address) form is complete/submitted.
- Ensure that Marines understand the following procedures/programs:
 - Family assistance.
 - Red Cross.
 - Casualty assistance.
 - Legal assistance.
 - The Soldiers and Sailors Relief Act.
- Ensure that TRICARE/DEERS information is updated and correct.
- Ensure that allotment to spouses/split pay is arranged.
- Ensure that dependent ID cards are current through date of return from deployment.
- Ensure that custody of children for single parents is legally established.
- Establish personnel database:
 - Name, rank, SSN, MOS.
 - Security clearance.
 - Meal card.
 - Weapon number.
 - Section.
 - Blood type.

- ID tags/cards.
- Next of kin.
- CPOG, gas mask size.
- Uniform, boot size.
- Updated record of emergency data (RED).
- Messman requirements.
- Corpsman request.
- Armory draw.
- Recall roster.
- Security for personal effects (supply).
- Banks/credit unions.
- Mortgage/deed of trust/financial obligations.
- Leases.
- Outstanding bills (address of creditors).
- Insurance coverage.
- Safe deposit box.
- Automobile storage.
- Storage of household goods.
- Right to vote.
- Memberships and subscriptions.

Logistics

Embarkation

- Determine equipment requirements.
- Determine logistical support requirements.
- Identify hazardous materials (HAZMAT) and storage/disposal procedures.
- Prepare personnel and equipment for embarkation.
- Obtain shipping lists.
- Identify and label embarkation boxes.
- Submit equipment density list (broken down by ship or transport relay).
- Determine transportation requirements (personnel).
- Waterproof materials.

- Prepare embarkation list for each box.
- Provide air and surface transport support equipment (height, length, weight, cube).
- Determine material handling equipment requirements (forklift/crane).
- Inspect vehicles, generators, HAZMAT.
- Prepare staging schedule (TPFDD).
- Prepare 463L pallet request/inventory (check for proper straps).
- Submit MilVan/ConEx/QuadCon requests.
- Determine requirement and understand procedures for HAZMAT, packaging, handling, storage, transportation, etc.

Supply

- Block of materials request.
- Camouflage netting requirements.
- Tentage.
- Cots.
- Field desks/tables/chairs.
- Meals, ready to eat (MREs).
- Training allowance pool gear.
- Batteries.
- Wire.
- Sandbags.
- Plastic.
- Flooring.
- Heaters.
- Schedule.

Utilities

- Determine power requirements.
- Submit generator (and operator) requests.
- Conduct generator operator license training.
- Provide light bulbs.
- Provide drip pans/fuel drums.
- Determine mobile electric power distribution system cabling/harness requirements.

Motor Transport

- Conduct HMMWV/five-ton license training.
- Determine convoy route.
- Submit vehicle and driver assignments (consideration: command group drivers).
- Determine convoy composition.
- Establish convoy communications/control procedures.
- Determine requirement for vehicle placards.
- Determine fuel requirements (petroleum, oils, and lubricants).
- Determine requirement for trip tickets.

Step 6. Transition

The last step in the MCPP is transition of the OPOD from the planners to the executors (at the MEF level, from future operations to current operations). The planning, decision, and execution cycle continues with planners responding to the developing situation and with new or revised missions.

Appendix H

Data Communications Network and Information Systems Planning Checklist

Gateway Access Coordination

- Determine bandwidth requirements (over 32 kbps will require special coordination).
- Incorporate request for NIPRNET/SIPRNET/JWICS into satellite access request.
 - MEF IP networks to be used.
 - Router type.
 - Encryption device.
 - Data rate.
 - Exterior routing and encapsulation protocol (i.e., BGP4/EGP and PPP/HDLC).
- Ensure standard gateway COMSEC (ICP USKAT: C5573).
- Coordinate/confirm KG-84A/C front-panel settings with gateway.
- Contact DISA, per mission directive, 7–10 days before scheduled activation to confirm IP addressing and routing information.
- Coordinate with the local information office, in conjunction with MEF G-6, to establish a NIPRNET server-to-server connection.
- Identify transmission system links to be used in support of data networks, in conjunction with communications battalion/squadron systems planning and engineering staff and the G-6.
- Identify data rates to subordinates.
- Determine the interior routing and encapsulation protocol to be used with subordinates (i.e., IGRP/OSPF and HDLC/PPP).
- Determine autoroute tables and related requirements for all JMCIS workstations.
- Determine CSU/DSU unit leased-line requirements.
- Determine the number of hosts (MEF CE) that require an IP address (UNIX TDS workstations and PCs configured as IP clients).
- Determine the appropriate IP subnet mask to be used.
- Design a detailed IP data network for NIPRNET, SIPRNET, and JWICS (MEF CE will provide IP addresses for MEF/subordinate IP interface).
- Determine the COMSEC keymat to be used (generally will use same as gateway).
- Coordinate DNS access/use, if required.

MEF WAN Requirements

- Determine the number of subordinate/adjacent commands/units requiring serial port router access.
- Determine appropriate router type.
 - CISCO 4000 (two serial/four Ethernet)
 - CISCO 7010 (eight serial/six Ethernet)

LAN Requirements

- Determine the number of PCs to be connected to each network.
- Determine the number of services required.
- Determine the number of TDSs to be connected to SIPRNET (e.g., GCCS, IAS, TCO, CTAPS, etc.).
- Identify the geographical area that the MEF CE will use (tents, buildings, or trailers) and the physical separation/distance between sections.

- Determine cabling and connector requirements (RG-58, fiber optic, thick Ethernet, BNC connectors, terminators, T connectors).
 - RG-58: maximum distance, 185 m.
 - Thick Ethernet: maximum distance, 500 m.
 - Fiber optic: maximum distance, 2.5 miles multi-fiber, 10 miles single fiber.
- Determine the number of repeaters required. (The number depends on the physical layout of the CE and number of PCs/laptops/TDSs.)
- Determine the number of servers required. (The number depends on applications: Plan for 1 server per 35 users when message distribution system (MDS) is being used.)
- Design a detailed LAN diagram with appropriate cable segments, repeater, routers, servers, TDSs, and IP clients identified.
- Determine server application requirements (e.g., MDS, e-mail, etc.).
- Determine the number of LAN dial-ins required and the type of interface (i.e., KY-68, STU-III, Hayes Modem).
- Determine the concept of operations for INFOS-EC monitoring and analysis, and initiate necessary support requests.
- Determine power requirements (generally, 15 kW, 120 V, 60 Hz).
- Determine the number of personnel required to support the exercise/operation. Keep in mind:
 - WAN monitoring/maintenance will generally require two Marines per shift.
 - The help desk will generally require one Marine per shift.
 - LAN troubleshooting will generally require 1 Marine per 35 computers per shift.
 - 24-hour operations require 12-hour shifts.
 - Duration of exercise/operation will affect personnel requirements.
- Submit COMSEC request to CMS.
- Coordinate priority DSN/INMARSAT access for initial SIPRNET/NIPRNET/JWICS installation.
- Coordinate one AN/GRA-39 per shelter. (When using HMMWV-mounted shelters, arrange for two.)
- Coordinate separate J1077 (J-box)/26-pair cable for data serial connections for each shelter (reduces conflicts with wire/telephone connections—recommended when supporting multiple serial line connections).

Logistic and Personnel Planning

- Determine block of materials requirements on the basis of requirements and preliminary planning, and submit 45–60 days before deployment.
- Determine embarkation requirements, including shelters to be used (height, weight, width, length), on the basis of equipment requirements and geographical location.
- Submit appropriate log requests for lifting and transporting shelters or pallets (if required).
- Determine power distribution and grounding requirements.

Network Management

- Coordinate IP address management in conjunction with principal staff officers and higher/ adjacent/subordinate unit communications and information systems officers.
- Create appropriate user accounts in accordance with Marine Corps and MEF standards, per G-6 input.
- Implement a virus management plan in conjunction with the G-6.
- Implement an automatic data processing security plan in conjunction with the G-6.
- Implement an internet access policy in conjunction with the G-6.

Preexercise Equipment Preparation

- Identify the equipment required to support the exercise/operation.
- Configure and test servers (see Server Checklist on page H-4).
- Configure and test routers and repeaters (see Router/Repeater Checklist on page H-5).
- Confirm proper crypto strappings.
- Inspect and test all KG-84 red and black side cables.
- Configure and test all CSU/DSU modems and cables.
- Preconfigure and bench test equipment string.
- Coordinate a data communications pretest/configuration exercise with subordinate units, if feasible.
- Ensure that all application, diagnostic, and server software is loaded on each server and on diskette (two copies), tape, or compact disk (CD).
- Ensure that all UPSs are tested.
- Ensure that all network and router management PCs/laptops are configured and tested properly.
- Ensure that all equipment is embarked in a manner that will minimize equipment damage.
- Ensure that appropriate backup equipment is tested and embarked.

SERVER CHECKLIST										Date _____
Server serial no. _____ Server key no. _____ Server name _____ Server console password _____ Sys admin account name: SysAdmin* _____ Password _____ Processor (min. 486) _____ RAM (min. 16 Mb) _____ Hard disk size (min. 500 Mb): No. 1 _____ No. 2 _____ No. 3 _____ Tape backup unit _____										
Network interface cards and intelligence communication adapter:					Services created:					
Slot	Type/Maker	IRQ	I/O Address	RAM Address	Init.	Started	Type	Name		
_____	_____	_____	_____	_____	_____	Started	File	SHARED FILES*		
_____	_____	_____	_____	_____	_____	Started	File	DATACOMM SHARED FILES*		
_____	_____	_____	_____	_____	_____	Started	ISMTTP	ISMTTP*		
_____	_____	_____	_____	_____	_____	Stopped	STDA	SATELLITE STDA*		
_____	_____	_____	_____	_____	_____	Stopped	Print	SHARED PRINTER*		
Server options:					Software installation (each program loaded and tested):					
Init.	Version No.				On SHARED FILES*					
_____	VINES operating system				Init.					
_____	Server-to-server LAN				_____	Lotus SmartSuite (LAN user)				
_____	Server-to-server WAN (HDLC)				_____	MTF Editor				
_____	PC print				_____	MDS				
_____	Asynchronous dial-in				_____	VDS				
_____	Asynchronous terminal emulation				_____	MCLLS				
_____	Mail service				_____	JULLS				
_____	Network management				On DATACOMM SHARED FILES*					
_____	VINES assistant toolbox				_____	MS-DOS				
_____	TCP/IP routing				_____	Windows				
_____	TCP/IP server to server				_____	ProComm Plus				
_____	Incognito simple mail transfer protocol (ISMTTP) (software only)				_____	3 Com Etherlink II Diag				
_____	Incognito domain name server (software only)				_____	3 Com Etherlink III Diag				
_____					_____	PCtools				
_____					_____	SuperTCP for Windows				
Server accessories:					Hardware test verification:					
Init.					Init.					
_____	Power cable (CPU, monitor, printer, router)				_____	Each network interface card tested with a client PC				
_____	UPS				_____	Intelligence communication adapter tested (each port)				
_____	ICA cables				_____	Floppy drive tested				
_____	Surge protectors (2)				_____	Tape backup tested and verified				
_____	Extension cord (15 ft. or more)				_____	Platform diagnostics run				
_____	Printer				_____	Last second echelon preventive maintenance _____				
_____	Printer cable				Next scheduled second echelon preventive maintenance _____					
_____	Printer ribbons/toner cartridge				*@servername@servers					
_____	Blank option key									
_____	Server software/CD-ROM									

ROUTER/REPEATER CHECKLIST			
Router CISCO 4000/7010			
Serial no. _____		Router name/no. _____ Router password _____	
Software version no. _____		Router configuration printed and attached _____ (initials)	
Router hardware verification (each port must be tested)		Ethernet transceivers and AUI cables (test each)	
Init.		Init.	Serial no.
_____ Serial 0	_____ Ethernet 0	_____ One transceiver per router/repeater port	_____
_____ Serial 1	_____ Ethernet 1	_____ One AUI cable per router/repeater port	_____
_____ Serial 2	_____ Ethernet 2	_____ Five backup transceivers/AUI cables	_____
_____ Serial 3	_____ Ethernet 3		
_____ Serial 4	_____ Ethernet 4		
_____ Serial 5	_____ Ethernet 5		
_____ Serial 6	_____ Ethernet 6		
_____ Serial 7	_____ Ethernet 7		
Repeater		Serial no. _____	
Quantity	Init.		
_____ AUI ports	_____ All ports tested		
_____ Ethernet ports	_____ One transceiver/AUI cable per AUI port, serial nos.: _____		
UPS (two)			
Init.			
_____ Tested good			
Additional items			
Init.	Quantity	Item	
_____	_____	Blank, option keys (five)	
_____	_____	Cable, AUI (five: one per router/repeater port)	
_____	_____	Cable, CISCO 4000 to RS-449	
_____	_____	Cable, CISCO 7010 to KG-84C	
_____	_____	Cable, power (CPU, monitor, router, repeater)	
_____	_____	Cable, RS-232 to KG-84 red (six per ICA)	
_____	_____	Cable, RS-449 to KG-84 red (four)	
_____	_____	ICA cable (one per ICA)	
_____	_____	Surge supresser (two)	
_____	_____	Transceiver, thinnet	

(reverse blank)

Appendix I

Communications and Information Systems Estimate

COMMUNICATIONS AND INFORMATION SYSTEMS ESTIMATE
(Local variations and modifications as necessary to meet requirements.)

CLASSIFICATION

Copy no. ____ of ____ copies

Issuing headquarters

PLACE OF ISSUE

Date/time of issue

COMMUNICATIONS AND INFORMATION SYSTEMS ESTIMATE

Ref:

1. () MISSION. (This subparagraph contains a brief restatement of the basic mission of the command as a whole as previously announced by the commander. Deduced missions necessary for the accomplishment of the basic mission, along with previous decisions of the commander regarding either deduced or basic missions should be listed in appropriate subparagraphs.)

2. () SITUATION AND CONSIDERATIONS.

a. () Intelligence Situation. (Information known or obtained from the G2. Where appropriate, reference may be made to the Intelligence Estimate or other intelligence documents.)

(1) () Characteristics of the Area. (Those affecting C2.)

(a) () Weather.

(b) () Terrain.

(c) () Transportation networks/communication routes.

(d) () Other area characteristics that affect C2.

(Page number)

CLASSIFICATION

CLASSIFICATION

- (2) () Enemy Strengths and Disposition of Major Units
 - (a) () Tactical units.
 - (b) () Signals intelligence/electronics warfare.
 - 1. () Jamming.
 - 2. () Wire tapping.
 - 3. () Imitative deception.
- b. () Friendly Forces. (Information obtained from the commander's planning guidance and from the G-3.)
 - (1) () Present Disposition of Major Units
 - (a) () Tactical units.
 - (b) () CIS elements.
 - (2) () Courses of Action to be Considered
 - (a) () Course of action #1.
 - (b) () Course of action #2, etc.
 - (3) () Projected Operations. (If known, and which will affect the CIS situation.)
 - (a) () Rates of advance.
 - (b) () Command post location and displacement.
 - (c) () Uncovering of major communication routes.
 - (d) () Other projected operations that affect the CIS situation.
- c. () Personnel Situation. (Information known or obtained from the G-1 regarding personnel matters affecting the CIS situation. Where appropriate, make reference to the personnel estimate or other personnel documents.)
 - (1) () Strengths.
 - (2) () Replacements.

(Page number)

CLASSIFICATION

CLASSIFICATION

- (3) () Command post organization and operation.
- (4) () Other personnel matters affecting the CIS situation.
- d. () Logistics Situation. (Information known or obtained from the G-4 regarding logistics matters affecting the CIS situation. Where appropriate, reference may be made to the logistics estimate or other logistics documents.)
 - (1) () Availability of equipment.
 - (2) () Condition of equipment.
 - (3) () Availability of repair parts and consumable items.
 - (4) () Other logistic matters affecting the CIS situation.
- e. () Assumptions. (Any assumptions required as a basis for initiating planning or for the preparation of the estimate.)
- f. () CIS Situation.
 - (1) () General. (Information regarding current communication installations, the status of the overall communications system, and the location and mission of communication and control agencies. Reference may be made to the CIS SOP and COI or to the command, control and communications systems annexes contained in current operation plans or orders.)
 - (2) () Special. (Items not covered elsewhere which affect the CIS situation.)
 - (a) () Availability and assignment of radio frequencies.
 - (b) () Assignment of call signs.
 - (c) () Availability of shipboard communication equipment for troop use.
 - (d) () Arrangements for communications guard.
 - (e) () Anticipated traffic volumes.
 - (f) () Cryptographic matters.
 - (g) () Other special items affecting the CIS situation.

(Page number)

CLASSIFICATION

CLASSIFICATION

3. () ANALYSIS. (Each course of action under consideration is analyzed in the light of significant factors to determine problems which will be encountered, measures required to solve such problems, and any limiting features which will exist.)

a. () Course of Action #1.

(1) () Support Requirements,

(a) () Terrain and Distance Factors. (A discussion of terrain and distance factors that may affect the location of command posts, installations, and the employment of communications means.)

(b) () Installations. (A discussion of known or deduced communications requirements for each communications and control agency and other units. These requirements may be expressed as need lines or may be detailed to include types of circuits and terminal service, or other forms of communications, required by these activities.)

(2) () Support Capability. (A discussion of the capability to employ all available means of communications to satisfy the foregoing support requirements.)

(a) () Radio and Wire. (Discussed in conjunction with the capability to provide various types of circuits and attendant terminal service; e.g., telephone, facsimile, and data.)

(b) () Network Systems.

(c) () Messenger.

(d) () Visual and Sound.

b. () Course of Action #2. (Same for each COA #1.)

4. () EVALUATION. (Based on the foregoing analysis, the advantages and disadvantages of each course of action are summarized and compared from a CIS viewpoint.)

a. () Course of Action #1.

(1) () Advantages.

(2) () Disadvantages.

(Page number)

CLASSIFICATION

CLASSIFICATION

- b. () Course of Action #2.
 - (1) () Advantages.
 - (2) () Disadvantages.
- c. () Other Courses of Action.
- 5. () CONCLUSIONS.
 - a. () COA Statement. (A statement as to which course of action under consideration can best be supported from a CIS viewpoint.)
 - b. () Salient Disadvantages Statement. (A statement of the salient disadvantages which render the other courses of action less desirable from a CIS viewpoint.)
 - c. () Significant Problems Statement. (A statement of significant CIS problems to be solved and limitations which may exist.)
 - d. () Resolution Statement. (A statement of measures required to resolve the foregoing CIS problems and offset any limitations which may exist.)

/s/ _____

Appendixes: (As appropriate)

Appendix J

Sample CIS Annex (Annex K)

The CIS annex generally follows the basic OPLAN or OPORD format. General instructions for preparation are provided below. A sample Annex K appears on pages J-4 through J-14.

Heading

The heading is the same as the heading of the OPLAN or OPORD and gives the following information:

Issuing HQ

This consists of the official designation of the command.

Place of Issue

This shows the physical location of the issuing HQ. All letters are capitalized.

Date-Time Group

This indicates the date and time the plan or order is signed and, unless otherwise specified in the plan or order, the date and time the annex becomes effective. It is expressed in standard military sequence: day, hour, minutes, time zone suffix, month, and year (e.g., 151200Z Jan 2000). The time zone used will be that of the operations area or universal coordinated time.

Designation and Title of the Annex

The title of an annex consists of a capital letter followed by an indication of the subject matter in parentheses and by the number of the OPLAN or OPORD to which it is attached.

References

Included in the heading and listed as references are other sources of information (CIS SOPs, CEOI, maps, charts, or overlays) needed to under-

stand the annex. The caption Ref:_____ is always included. When there are no references, the caption will be followed by the word "none." Each item cited as a reference is preceded by a letter in parentheses and is in alphabetical sequence (e.g., (a), (b), etc.). Information regarding maps and charts should include the country, scale, name and sheet number, and year of edition, or the appropriate information required to locate them on compact disc.

Time Zone

The time zone normally used in the plan or order is that of the objective area. When the plan or order applies to units in different time zones, universal coordinated time or the time specified by higher HQ is used.

Body

The body of the annex contains information consistent with that contained in the main body but focused on information relevant to CIS.

General

This subparagraph contains a brief, general statement of the purpose of the annex with respect to the basic plan objectives. It provides guidance for CIS support of the operation.

Situation

This paragraph provides an overview of the environment in which the CIS support described in the annex will be provided. This includes the reason for the annex, the friendly and enemy situation, and assumptions that are necessary to planning. This subparagraph summarizes the situation consistent with that of the main body, but focusing on those factors that affect CIS.

General. This subparagraph will make reference to the concept of operations.

Enemy Forces. This subparagraph contains enemy forces information that will affect CIS employment. This subparagraph usually references the intelligence annex or provides specific information on the enemy's intelligence, EW, or deception (or other) capabilities; C2 facilities; CIS capabilities; and the possible exploitation of enemy assets.

Friendly Forces. This subparagraph contains information on the higher, adjacent, supported, and/or supporting units or facilities involved in the C2 support of the operation. This subparagraph identifies communications elements attached or detached for the operation. Reference may also be made to the task organization annex.

Assumptions. This subparagraph establishes essential criteria for developing the CIS annex. If, as the planning phase progresses and the situation develops, the assumptions prove mistaken, then the plan must be modified accordingly. Assumptions define the anticipated conditions that will drive CIS requirements and affect CIS capabilities; they are major considerations for planning CIS support. The number of assumptions should be held to a minimum and worded carefully to describe concisely and accurately the conditions on which the plan is based. Assumptions are applicable to plans only.

Mission

This paragraph is a concise statement of the mission of the command. It should include the commander's intent and identify actions necessary to support this intent, the concept of operations, and the commander's planning guidance. Normally, this paragraph states the time that the C2 facilities will commence and terminate operations.

Execution

Guiding Principles

This subparagraph outlines the principles necessary for the coordination and guidance of all commands and units. Selected policies, doctrine, or

procedures that are contained in the references but that need emphasis are called out. New procedures are included in a separate subparagraph.

Operational Concept

This subparagraph describes briefly how the entire operation is visualized from the CIS viewpoint. Particular emphasis is placed on aspects of the basic plan that establish CIS support requirements, capabilities, and limitations.

Tasks and Responsibilities

This subparagraph assigns specific CIS support missions or tasks for both issuing and subordinate units. The tasks for each unit are addressed in separate subparagraphs. In addition, instructions for functional areas such as intelligence, fires, and logistics are in specific subparagraphs and often expanded on in appendices to Annex K. It should be noted that CIS support for functional areas is also routinely incorporated into CIS appendices, tabs, or enclosures that are a part of the OPLAN/OPORD annexes covering those functional areas.

Coordinating Instructions

This subparagraph provides instructions for CIS support tasks that apply to two or more units.

Special Measures. This paragraph is separated into subparagraphs and provides information regarding each special measure or procedure necessary to support the mission that is not addressed above or in paragraph 4 of the OPLAN or OPORD. This paragraph includes specific information pertaining to measures such as routing indicators, electronic identification procedures, and liaison teams.

Information Management. This paragraph provides instructions for ensuring that the communications and information management systems supports the unit information management plan. Usually, this paragraph references the annex that addresses CIS support for information management.

Administration and Logistics

Administration

This paragraph contains administrative procedures concerning CIS support in the areas of personnel,

records, reports, and other administrative matters. It will include identification of CPs ashore and afloat.

Logistics

This paragraph contains logistics information relating to CIS employment, and usually references the logistic/CSS annex.

Command and Control

Command Relationships

This paragraph contains information relating to command relationships and usually refers to the appropriate appendices in the OPORD.

Communications and Information Systems Plans

This paragraph refers to the appropriate appendices in the OPORD.

Ending

The ending of the CIS annex consists of the following:

- Acknowledgment instructions.

- Signature of either the commander or the commander's authorized representative. (Authentication by the authorized representative is also acceptable.)
- List of the appendices attached to the annex.
- Distribution.

Appendices

Appendices amplify information contained in the basic CIS annex and are used to promote accuracy, brevity, and clarity. The material contained in the appendices is usually technical, detailed, and complex in nature. The information often lends itself to presentation in tabular, schematic, or overlay form. MCWP 5-1 (draft) provides amplifying information. Typical appendices that may be prepared to support the basic CIS annex include communications security, call signs, visual and sound communications, and frequency management, to name but a few possibilities. The sample format (pages J-4 through J-14) contains a more extensive listing of possible appendices, but the listing provided is not meant to be either exhaustive or mandatory. The number and type of appendices required will vary with the situation and the needs of the preparing organization.

CLASSIFICATION

Copy no. _____ of _____ copies
 Issuing headquarters
 PLACE OF ISSUE
 Date/time of issue
 Message reference number

ANNEX K TO (UNIT) OPOD (NUMBER) (U)**COMMUNICATIONS AND INFORMATION SYSTEMS (U)**

- (U) Ref: (a) MCWP 6-22 (Communications and Information Systems) (U)
 (b) CJCSM 6231 (Series) (Manual for Employing Tactical Communications) (U)
 (c) ACP 121 (Communications Instructions—General) (U)
 (d) ACP 122 (Series) (Communications Instructions—Security) (C)
 (e) ACP 167 (Series) (Glossary of Communications-Electronics Terms) (U)
 (f) NWP 4 (Series) (Basic Operational Communications Doctrine) (U)
 (g) NTP-3 (Series) (Telecommunications—Users Manual) (U)
 (h) NTP-4 (Series) (Naval Telecommunications Procedures—Fleet Communications) (C)
 (i) NTP-5 (Voice Communications) (U)
 (j) JANAP 128 (Series) (Automated Digital Network (AUTODIN) Operating Procedures) (U)
 (k) (Higher Headquarters) (Communication and Information Systems Plan) ()
 (l) (Higher Headquarters) (OPOD) ()
 (m) (Unit) Order (Communication and Information Systems SOP) ()
 (n) (Unit) Order (Information Management SOP) ()

(U) Time Zone: Z

1. () GENERAL. This annex provides guidance for employing CIS architecture to support (unit) operations.

2. () SITUATION.

a. () General. (See Concept of Operations, Annex C (Operations))

b. () Enemy.

(1) () See Annex B (Intelligence)

(2) () The enemy has the capability to—

(Page number)

CLASSIFICATION

CLASSIFICATION

- (a) () Conduct satellite-based EA, including imitative communications deception, jamming (both communications and radar), radar deception, and electromagnetic virus insertion operations.
 - (b) () Intercept, analyze, and report timely intelligence information derived from friendly emitters to appropriate enemy commanders.
 - (c) () Accurately locate and target friendly forces communications and electronic emitters by DF.
 - (d) () Conduct meaconing operations against both TACAN and low-frequency automatic direction finding (ADF) navigation receivers.
 - (e) () Access and gain temporary control of commercial digital telecommunications switches and deny access to satellite communications switches in geosynchronous orbit.
 - (f). () Employ malicious logic techniques against our information systems.
- c. () Friendly. See Annex A (Task Organization).
- (1) () Higher headquarters or other specific organizations that will provide CIS to (unit) in a specific operation.
 - (2) () The command relationship between friendly forces is shown in Annex J (Command Relationships) to this OPORD.
 - (3) () Attachments and Detachments
 - (a) () (See Annex A (Task Organization) to this OPORD.
 - (b) () When OPCON is taken of MAGTF units as (unit) forms during compositing, MARFOR CIS assets will be listed separately.
- d. () Assumptions. (State the assumptions that establish essential criteria for development of the annex.)
3. () MISSION. Commencing and terminating on order, (unit) communications organizations provide, install, operate, and maintain the internal and external communications and support the installation, operation, and maintenance of information systems for reliable C2.

(Page number)

CLASSIFICATION

CLASSIFICATION

4. () EXECUTION

a. () Commander's Intent. Synopsis of the commander's intent that bears on employing CIS.

b. () Guiding Principles

(1) () The procedures contained in references (a) through (n) will be used.

(2) () (Unit) operations will be conducted in a hostile EW environment. The following degradations are to be expected.

(a) () Loss of DCS entry due to equipment damage or circuit path loss.

(b) () Isolation of a headquarters due to loss of wideband systems.

(c) () Hostile interference on all terrestrial/satellite MCR and SCR systems (jamming).

(d) () Loss of a switchboard due to component failure or hostile action.

(e) () Loss of a satellite asset due to EW or destruction of the satellite.

(f) () Disruption or loss of information systems due to component failure or hostile action.

(3) () Frequency changes, radio transmission brevity, and, on occasion, complete EMCON will be employed in order to facilitate control and reduce anticipated interference with communications.

(4) () Backup CIS equipment and alternate communications paths will be planned and installed to enhance reliability, flexibility, and responsiveness of CIS networks.

(5) () Based on coordination with affected commanders and principal staff officers, radio nets will be combined/pooled at the COCs and other C2 facilities to conserve the frequency spectrum and reduce communications requirements.

(6) () Information systems security and COMSEC measures will be employed to deny information of value to the enemy and to prevent loss or disruption of service through hostile action. Refer to Appendix 1 (Communications and Information Systems Security) to this annex for details.

(Page number)

CLASSIFICATION

(CLASSIFICATION)

(7) () The (unit) G-6/S-6 will be the single point of contact at this headquarters for obtaining CIS services, support, or interface with higher headquarters, NTS, DISA, or other external agencies.

c. () Operational Concept

(1) () Every means available will be used to provide the commander with the ability to exercise C2 and to accomplish the assigned mission. It is the responsibility of the G-6/S-6 to make the commander fully aware of the capabilities and limitations of available CIS.

(2) () Subordinate unit CIS officers must advise the G-6 of situations, actual or potential, that could adversely affect MAGTF CIS support.

(3) () The major limitation of the CIS network is the EW threat. The enemy has the full capability to disrupt, intercept, and confuse friendly forces CIS operations. Line-of-sight communications will be adversely affected because of extremely rugged terrain throughout the AO.

(4) () The critical vulnerability of CIS network is the degradation of the common tactical picture during extended COC and CP displacements.

(5) () The COG of the CIS network is the capability to adapt and scale the network through extensive retransmission and backup systems configurations. This provides full support of maneuver, intelligence, fires, CSS, and force protection throughout the AO.

(6) () Appendix 1 (Communications and Information Systems Security) to this annex lists measures designed to deny information to unauthorized persons.

(7) () Appendix 2 (Command and Control Protection) to this annex describes measures to ensure continuous availability of friendly CIS.

d. () Tasks and Responsibilities. Appendix 3 (Communications and Information Systems Planning) to this annex highlights CIS planning considerations for effective execution of the assigned mission.

(1) () (Communications Unit)

(a) () Provide the net control station(s) for all (unit) controlled radio circuits. See Appendix 4 (Radio Circuit Plan) to this annex.

(Page number)

CLASSIFICATION

CLASSIFICATION

- (b) () Ensure that information on call signs and routing indicators is promulgated to using staff sections/functional agencies. See Appendix 5 (Call Signs and Routing Indicators) to this annex.
 - c) () Install, operate, and maintain wire and MCR communications as described in Appendix 6 (Wire and Multichannel Radio Plan) to this annex.
 - (d) () Install, operate, and maintain the data communications network as described in Appendix 7 (Data Communications Network Plan) to this annex.
 - (e) () Promulgate visual and sound signals for the operation. See Appendix 8 (Visual and Sound Communications) to this annex.
 - (f) () Install, operate, and maintain a SYSCON and TECHCON facility in support of the (unit) communications networks. See Appendix 9 (Communications Control) to this annex.
- 1. () Ensure that a liaison representative is at higher and adjacent headquarters to facilitate the direct handling of questions and/or problems relating to CIS.
 - 2. () Ensure that the G-6/S-6 and appropriate watch officers are informed of the communications circuit status.
 - 3. () Ensure strict compliance with G-6/S-6 assigned frequencies. See Appendix 10 (Frequency Management) to this annex.
 - 4. () Ensure that the established power distribution system is properly grounded and that backup mobile power is available as necessary. See Appendix 11 (Power Requirements) to this annex.
 - 5. () Ensure that CP displacements are hastily executed with the requisite communications network scaled to retain essential information flow. See Appendix 12 (Command Post Displacement Communications) to this annex.
 - 6. () Ensure that the TACSAT communications are installed, operated, and maintained as depicted in Appendix 13 (Tactical Satellite Communications) to this annex.
 - 7. () Ensure that communications restoration is handled expeditiously. See Appendix 14 (Communications Restoration) to this annex.

(Page number)

CLASSIFICATION

CLASSIFICATION

8. () Ensure that the G-6/S-6 and the command are kept informed about the status of the commercial (local civilian) telecommunications systems.
- (g) () Install, operate, and maintain a communications and electronics maintenance facility to inspect, repair, and/or replace faulty communications and electronics equipment. See Appendix 15 (Special Maintenance Procedures) to this annex.
- (h) () Establish and maintain messenger service, including truck, helicopter, and motorcycle couriers, as directed in Appendix 16 (Messenger Service) to this annex.
- (i) () Install, operate, and maintain a communications center to support (unit) with over-the-counter service for all Marine units/agencies at the (unit) headquarters. See Appendix 17 (Communications Center) to this annex.
- (j) () Establish emergency action procedures for use in the communications center and any other area containing classified and/or cryptographic material. See Appendix 18 (Emergency Action) to this annex.
- (2) () Radio battalion/SSU: Install, operate, and maintain MAGTF CE special security communications terminal facilities.
- (3) () Ground Combat Element
- (a) () Install, operate, and maintain internal and external communication circuits and information systems as directed in unit SOPs and this annex.
- (b) () Be prepared to assume communications and crypto-guard for (unit(s)) and to assume net control of (unit) circuits in the event (unit) headquarters becomes a casualty.
- (c) () Install, operate, and maintain a SYSCON/TECHCON facility to ensure the rapid restoration/rerouting of communications circuits.
- (4) () Aviation Combat Element
- (a) () Install, operate, and maintain internal and external communications circuits and information systems as directed in unit SOPs and this annex.

(Page number)

CLASSIFICATION

CLASSIFICATION

- (b) () Install, operate, and maintain a SYSCON/TECHCON facility to ensure the rapid restoration/rerouting of communications circuits.
- (c) () Be prepared to maintain TADIL A, TADIL B, TADIL J, AT-DL-1, GBDL, and Link 1 connectivity with (fleet), (joint Service), and NATO agencies.
- (d) () Ensure the necessary liaison to establish and maintain the necessary MACCS interface with joint, other-Service, national, and international agencies, as required.
- (5) () Combat Service Support Element. Install, operate, and maintain a SYSCON/TECHCON facility to ensure the rapid restoration/rerouting of communications circuits.
- e. () Intelligence and Reconnaissance. State intelligence and reconnaissance support required even though they have been covered in Annexes B and C because Annex K may be distributed separately. If the information is very detailed, prepare an appendix to the CIS systems annex. If MILSATCOM is a requirement, ensure it's covered in Appendix 13.
- f. () Coordinating Instructions
 - (1) () Special Measures
 - (a) () The G-6/S-6 will make special efforts to indoctrinate staff/command personnel in alternate routes/means of communications to preclude the confusion or delay of information due to outages in the high-threat EW environment.
 - b) () The communications support for linkup operations is found in Appendix 19 (Communications for Linkup Operations) to this annex.
 - ((c) () Specific communications procedures relative to air assets are found in Appendix __ (Air Communications) to Annex __ (Air Operations) to this OPORD.
 - (d) () Safety is paramount in working with CIS. Appendix 20 (Safety) to this annex identifies major safety measures and concerns.
 - e) () Emergency evacuation operations require unique communications capabilities. See Appendix 21 (Noncombatant Evacuation Operations Communications) to this annex.

(Page number)

CLASSIFICATION

CLASSIFICATION

- (f) () Detailed instructions for the ITSDN/DISN/DCS STEP procedures are found in Appendix 22 (ITSDN/DISN/DCS) to this annex.
- (g) () Detailed instruction designed to alleviate confusion in the rapid task organization of (unit), with its necessary command communications support shifts, is found in Appendix 23 (Task Organization/Communications Guard Shifts) to this annex.
- (h) () The description for handling emergency action communications is found in Appendix 24 (Emergency Action Communications) to this annex.
- (i) () To alleviate confusion and to aid in the organized assignment of resources while embarked, Appendix 25 (Communications and Information Systems Support for Embarked Units) to this annex details assets available for (unit) use.
- (j) () Details for radio battalion/special security officer (SSO) communications support are found in Appendix 26 (RadBn/SSO Communications Support) to this annex.
- (k) () Procedures for effecting a reliable communications network in geographic areas in which climatic conditions require special consideration are found in Appendix 27 (Special Climatic/Geographic Considerations) to this annex.
- (l) () Special considerations for establishing and coordinating joint Service communications support are found in Appendix 28 (Joint Service Communications Coordination) to this annex.
- (m) () Instructions for establishing and coordinating communications connectivity with and in the host nation are found in Appendix 29 (Host Nation Communications) to this annex.
- (n) () Special communications considerations necessary to support hardback (information pull) and connectivity to global information systems are found in Appendix 30 (Global Communications) to this Annex.
- (o) () Special instructions for establishing and coordinating communications support for intelligence activities are found in Appendix 31 (Communications Support for Intelligence) to this annex.

(Page number)

CLASSIFICATION

CLASSIFICATION

(p) () Specific communications support relative to intelligence operations is addressed in Appendix 31 (Communications Support for Intelligence) to this annex.

(q) () Instructions for the establishment of Internet Protocol (IP) addresses are found in Appendix 34 (IP Address Assignments) to this annex.

(2) () Information Management. This paragraph contains instructions to ensure that employing CIS is coordinated with and supports the unit information management plan. Detailed instructions will be addressed in Appendix 35 to this annex.

5. () ADMINISTRATION AND LOGISTICS.

a. Administration.

(1) () Required CIS status and other reports are listed in Appendix 32 (Reports) to this annex.

(2) () Security violations will be reported in accordance with Appendix 1 (Communications and Information Systems Security) to this annex.

(3) () Procedures to support the administrative formation of a unit at sea are found in Appendix 33 (Compositing) to this annex.

(4) () CPs

MEF main: Vicinity (location). See reference (n) and Annex C (Operations).

*List remaining MEF and other subordinate elements' tactical, main, and rear echelons.

b. () Logistics

(1) () See Annex D (Logistics/Combat Service Support).

(2) () Units will deploy with the capability to perform basic organizational and field maintenance.

(3) () The service support unit will provide intermediate maintenance (direct support and general support) of all ground-common communications and electronics equipment.

(Page number)

CLASSIFICATION

CLASSIFICATION

(4) () Water, billeting, messing, and generator fuel will be provided by the unit that hosts multichannel teams.

(5) () Communications units deploy with sufficient maintenance equipment; repair parts (class IX); petroleum, oils, and lubricants (Class III); batteries; and cable for () days/weeks of sustained operations.

(6) () Report maintenance problems for critical low-density items to the G-6/S-6 immediately.

6. () COMMAND AND CONTROL

a. () Command Relationships. Refer to Annex J for command relationships.

b. () CIS Plans. All subordinate commands down to battalion level submit unit CIS plans to this headquarters (Attn: AC/S G-6) NLT (date).

T.U. STARR

Major General, U.S. Marine Corps
Commanding

Appendices:

- 1 Communications and Information Systems Security
- 2 Command and Control Protection
- 3 Communications and Information Systems Planning
- 4 Radio Circuit Plan
- 5 Call Signs and Routing Indicators
- 6 Wire and Multichannel Radio Plan
- 7 Data Communications Network Plan
- 8 Visual and Sound Communications
- 9 Communications Control
- 10 Frequency Management
- 11 Power Requirements
- 12 Command Post Displacement Communications
- 13 Tactical Satellite Communications
- 14 Communications Restoration
- 15 Special Maintenance Procedures
- 16 Messenger Service
- 17 Communications Center

(Page number)

CLASSIFICATION

CLASSIFICATION

- 18 Emergency Action
- 19 Communications for Linkup Operations
- 20 Safety
- 21 Noncombatant Evacuation Operations Communications
- 22 ITSDN/DISN/DCS
- 23 Task Organization/Communications Guard Shifts
- 24 Emergency Action Communications
- 25 CIS Support for Embarked Units
- 26 RadBn/SSO Communications Support
- 27 Special Climatic/Geographic Considerations
- 28 Joint Service Communications Coordination
- 29 Host Nation Communications
- 30 Global Communications
- 31 Communications Support for Intelligence
- 32 Reports
- 33 Compositing
- 34 IP Address Assignments
- 35 CIS Support for Information Management

OFFICIAL:

O.N.E. EAGLE
Colonel, USMC
AC/S G-6

DISTRIBUTION:

Appendix K

CIS Threat Assessment Planning Checklist

This checklist is designed to assist C2 planners in evaluating any threat capability to exploit and/or disrupt our CIS. Planners must understand the threat to develop a C2 architecture that performs effectively with minimum disruption.

Physical Destruction

- What type of weapons of mass destruction does the enemy have?
- Do they have antiradiation munitions? How accurate are they?
- What means of delivery of munitions are available?
- Do they have trained saboteurs? Infiltrators?
- What other means of physical destruction do they possess?
- Where are we most vulnerable to ground attack?
- Does the enemy possess and train to use chemical and biological agents? What are their means of delivery?
- Are lasers used against CIS targets?

Collection Systems

- Is the threat capable of—
 - Visible light, infrared imagery?
 - Electronic surveillance, direction finding?
 - Interception of radio signals, wiretapping?
 - Gathering HUMINT and placing agents in the area?

- What means of collection are used?
 - Satellite? What is the footprint? When are we most vulnerable?
 - Overflights? What platforms are used? What capability do they have?
 - Ground collection units? Where? Capability? Range of their equipment? What frequencies? Is it a part of a worldwide collection and reporting network?
- How is information used and distributed?
 - Direct targeting?
 - Tracking?
 - Intelligence analysis?

Jamming

- What type of jamming do they use? Barrage? Spot?
- What frequencies are vulnerable?
- What geographic area is likely to be affected?
- What equipment do they use? How is it deployed?
- What techniques are most likely to be used?
- What circuits are most vulnerable?

Imitative Deception

- Level of sophistication?
- Do they have trained imitative communications deception operators?
- How do they deploy?
- What techniques have they used in the past?

(reverse blank)

Appendix L

Emission Classification and Designation

The International Telecommunication Union (ITU) at its World Administrative Radio Conference in 1979 in Geneva, Switzerland, adopted an international standard method of forming radio emission designators. Emissions shall be designated according to their necessary bandwidth and their classification character as prescribed by the ITU. Information about the character codes in this appendix is derived from the *Manual of Regulations and Procedures for Federal Radio Frequency Management* (also referred to as the Redbook or NTIA Manual), pages 9-16 through 9-18. The current version of this manual is available on the National Telecommunications and Information Administration (NTIA), Department of Commerce, Web page: www.ntia.doc.gov or with the frequency manager.

Necessary Bandwidth

For a given class of emission, the width of the frequency band is just sufficient to ensure the transmission of information at the rate and with the quality required under specified conditions. The necessary bandwidth shall be added just before the classification symbols and shall be expressed by three numerals and one letter. The letter occupies the position of the decimal point and represents the unit of bandwidth. The first character shall be neither zero nor K, M, or G. Necessary bandwidths are expressed as follows:

Between 0.001 and 999 Hz shall be expressed in Hz (letter H). Examples:

0.002 Hz = H002	25.3 Hz = 25H3
0.1 Hz = H100	400.0Hz = 400H

Between 1.00 and 999 kHz shall be expressed in kHz (letter K). Examples:

2.4 kHz = 2K40	180.4 kHz = 180K
6.0 kHz = 6K00	180.5 kHz = 181K
12.5 kHz = 12K5	180.7 kHz = 181K

Between 1.00 and 999 MHz shall be expressed in MHz (letter M). Examples:

1.25 MHz = 1M25	10.0 MHz = 10M0
2.0 MHz = 2M00	202 MHz = 202M

Between 1.00 and 999 GHz shall be expressed in GHz (letter G). Example:

5.65 GHz = 5G65

Classification

Emissions shall be classified and symbolized according to their basic characteristics. Optional characteristics may be used. Normally, only the basic characteristics are required.

Basic Characteristics

- First character—type of modulation of the main carrier.
- Second character—nature of signal(s) modulating the main carrier.
- Third character—type of information to be transmitted.

Modulation that is used only for short periods and for incidental purposes (such as, in many cases, for identification or calling) may be ignored provided the necessary bandwidth as indicated is not thereby eased.

First Character

Unmodulated

Emission of an unmodulated carrier

<u>Character</u>	<u>Description</u>
N	Unmodulated carrier

Amplitude Modulated

Emission in which the main carrier is AM (including cases where subcarriers are angle modulated).

<u>Character</u>	<u>Description</u>
A	Double sideband
H	Single sideband, full carrier
R	Single sideband, reduced or variable-level carrier
J	Single sideband, suppressed carrier
B	Independent sidebands
C	Vestigial sideband

Angle Modulated

Emission in which the main carrier is angle modulated.

<u>Character</u>	<u>Description</u>
F	FM
G	Phase modulation

Amplitude and Angle Modulated

CE mission in which the main carrier is amplitude and angle modulated, either simultaneously or in a preestablished sequence.

<u>Character</u>	<u>Description</u>
D	Amplitude and angle modulation

Pulse

Emission of pulses (emissions for which the main carrier is directly modulated by a signal that has been coded into quantized form (e.g., pulse-code modulation)), should be designated using the characters listed above in amplitude modulated, or angle modulated.

<u>Character</u>	<u>Description</u>
P	Sequence of unmodulated pulses
K	Modulated in amplitude
L	Modulated in width/duration
M	Modulated in position/phase
Q	In which the carrier is angle modulated during the period of the pulse
V	That is a combination of the foregoing or is produced by other means
W	Of cases not covered above, in which an emission consists of the main carrier modulated either simultaneously or in a combination of two or more of the following modes: amplitude, angle, pulse
X	In cases not otherwise covered (A fully explanation for this selection must be provided in supplementary details)

Second Character

<u>Character</u>	<u>Description</u>
0	No modulating signal
1	A single channel* containing quantized or digital signal information without the use of a modulating subcarrier (this excludes time-division multiplex)
2	A single channel* containing quantized or digital signals with the use of a modulating subcarrier (this excludes time-division multiplex)
3	A single channel* containing analog signals
7	Two or more channels* containing quantized or digital signals
8	Two or more channels* containing analog signals
9	Composite system with one or more channels containing quantized or digital signals together with one or more channels containing analog signals
X	In cases not otherwise covered (a full explanation for this selection must be provided in supplementary details)

*In this context, the word “channel(s)” refers to the radio frequency channel.

Third Character

<u>Character</u>	<u>Description</u>
N	No information transmitted
A	Telegraphy for aural reception
B	Telegraphy for automatic reception

Character

Description

C	Facsimile
D	Data transmission, telemetry, and telecommand (The character D indicates that data, telemetry, or telecommand information* is being transmitted individually or that any combination of the three is being transmitted simultaneously. If any combination is being transmitted simultaneously, one of the multichannel symbols 7, 8, or 9 must be used for the second character.)
E	Telephony (including sound broadcasting)
F	Television (video)
W	Combination of the above (Use only for multichannel systems that have the capability to transmit all information* simultaneously.)
X	Cases not otherwise covered (A full explanation is required in supplementary details.)

*In this context, the word “information” does not include information of a constant, unvarying nature such as is provided by standard frequency emissions, continuous wave, and pulse radars

Optional Characteristics

The optional additional characteristics not normally required are—

- Fourth character—details of signal(s)
- Fifth character—nature of multiplexing

Fourth Character

<u>Character</u>	<u>Description</u>
A	Two-condition code with elements of differing numbers and/or durations
B	Two-condition code with elements of the same number and duration without error correction
C	Two-condition code with elements of the same number and duration with error correction
D	Four-condition code in which each condition represents a signal element (of one or more bits)
E	Multicondition code in which each condition represents a signal element (of one or more bits)
F	Multicondition code in which each condition or combination of conditions represents a character
G	Sound of broadcasting quality (monophonic)
H	Sound of broadcasting quality (stereophonic or quadraphonic)
J	Sound of commercial quality (excluding categories of sound given under characters K and L, below)

Character

Description

K	Sound of commercial quality with the use of frequency inversion or band splitting
L	Sound of commercial quality with separate FM signals to control the level of demodulated signal
N	Monochrome
O	Color
P	Combination of the above
Q	Cases not otherwise covered

Fifth Character

Character

Description

N	None
C	Code-division multiplex (this includes bandwidth-expansion technique)
F	Frequency-division multiplex
T	Time-division multiplex
W	Combination of frequency-division multiplex and time-division multiplex
X	Other types of multiplexing

Appendix M

Sample Guard Charts

LEGEND: X = GUARD W = WHEN DIRECTED A = AS REQUIRED M = MONITOR C = NET CONTROL	JOINT AIR COORDINATION NET	JOINT AIR COORDINATION NET	TACTICAL AIR DIRECTION NET	JOINT AIR SUPPORT COORDINATION NET	JOINT AIR SUPPORT COORDINATION NET	TADIL A (LINK 11)	TADIL B (LINK 11B)	JOINT ICN	JOINT TSN	JOINT DCN	JOINT VPN	JOINT TACTICAL AIR REQUEST	AIR TRAFFIC CONTROL	JOINT SAR NET	TADIL C (LINK 4A)	JMS	ATDL-1	NADGE (NATO LINK 1)
SOP CIRCUIT DESIGNATIONS	AC-1	AC-1A	AC-4	AC-10A	AC-10B	AC-11	AC-13	AC-14	AC-15	AC-16	AC-17	AC-18	AC-22	JTF-17	NONE	NONE	NONE	NONE
TRANSMISSION TYPE: 1=HF 3=UHF 2=VHF 4=UHFSATCOM	4	1	3	2	1	1 OR 3	↑	1	1	1	3	1	2 OR 3	1	3		↑	↑
CJTF/JFACC	C	C	C	C	C	X		C	C	X	C	C		C				
USMC TACC	X	W	X	X	X	X		X	X	X	X	X	X	M				
USMC TAOC						X		X	X	X	X		X		X			
USMC DASC			X									X		M				
USMC VMFA SQUADRONS															X			
USN NTDS SHIPS						X		X	X	X	X		X	M	X			
USN ATDS SHIPS						X	ROUTED THROUGH THE MULTICHANNEL NETWORK	X	X	X	X		X	M	X		ROUTED THROUGH THE MULTICHANNEL NETWORK	ROUTED THROUGH THE MULTICHANNEL NETWORK
USN FIGHTER/ ATTACK SQDNS															X			
USAF CRC				X	X	X		X	X	X	X	X	X	M		X		
USAF AOC						X				X				M			ROUTED THROUGH THE MULTICHANNEL NETWORK	ROUTED THROUGH THE MULTICHANNEL NETWORK
USAF AWACS						X		X	X	X						X		
USAF FACP			A									X						
USA FDC																X	ROUTED THROUGH THE MULTICHANNEL NETWORK	ROUTED THROUGH THE MULTICHANNEL NETWORK
							↓										↓	↓

Figure M-1. Sample Radio Guard Chart.

LEGEND: X = GUARD W = WHEN DIRECTED A = AS REQUIRED M = MONITOR C = NET CONTROL	MARFOR CMD NET	MARFOR TAC NET	MARFOR INTEL NET	MARFOR COMM COORD	MEF CMD NET 1	MEF CMD NET 2	MEF TAC 1	MEF TAC 2	MEF ALERT BRDCAST	MEF INTEL 1	MEF INTEL 2	MEF CSS	MEF COMM COORD 1	MEF COMM COORD 2	TAR/HR 1	TAR/HR 2		
SOP CIRCUIT DESIGNATIONS	NONE	NONE	NONE	NONE	712A	712B	713A	713B	715	717A	717B	721	751A	751B	NONE	NONE		
TRANSMISSION TYPE: 1=HF 3=UHF 2=VHF 4=UHFSATCOM	AS DIR	AS DIR	AS DIR	AS DIR	1 OR 4	1	2	1	1	2	1	1	2	1	1	2		
MARFOR HQ	C	C	C	C														
MEF HQ	X	X	X	X	C	C	C	C	C	C	C	X	C	C	X	X		
MAW TACC					X	W	X	W	X	X	W	X	X	A	W	W		
MAR DIV HQ					X	W	X	W	X	X	W	X	X	A	X	X		
FSSG HQ					X	W	X	W	X	X	W	C	X	A	W	W		
DASC															C	C		

Figure M-1. Sample Radio Guard Chart (continued).

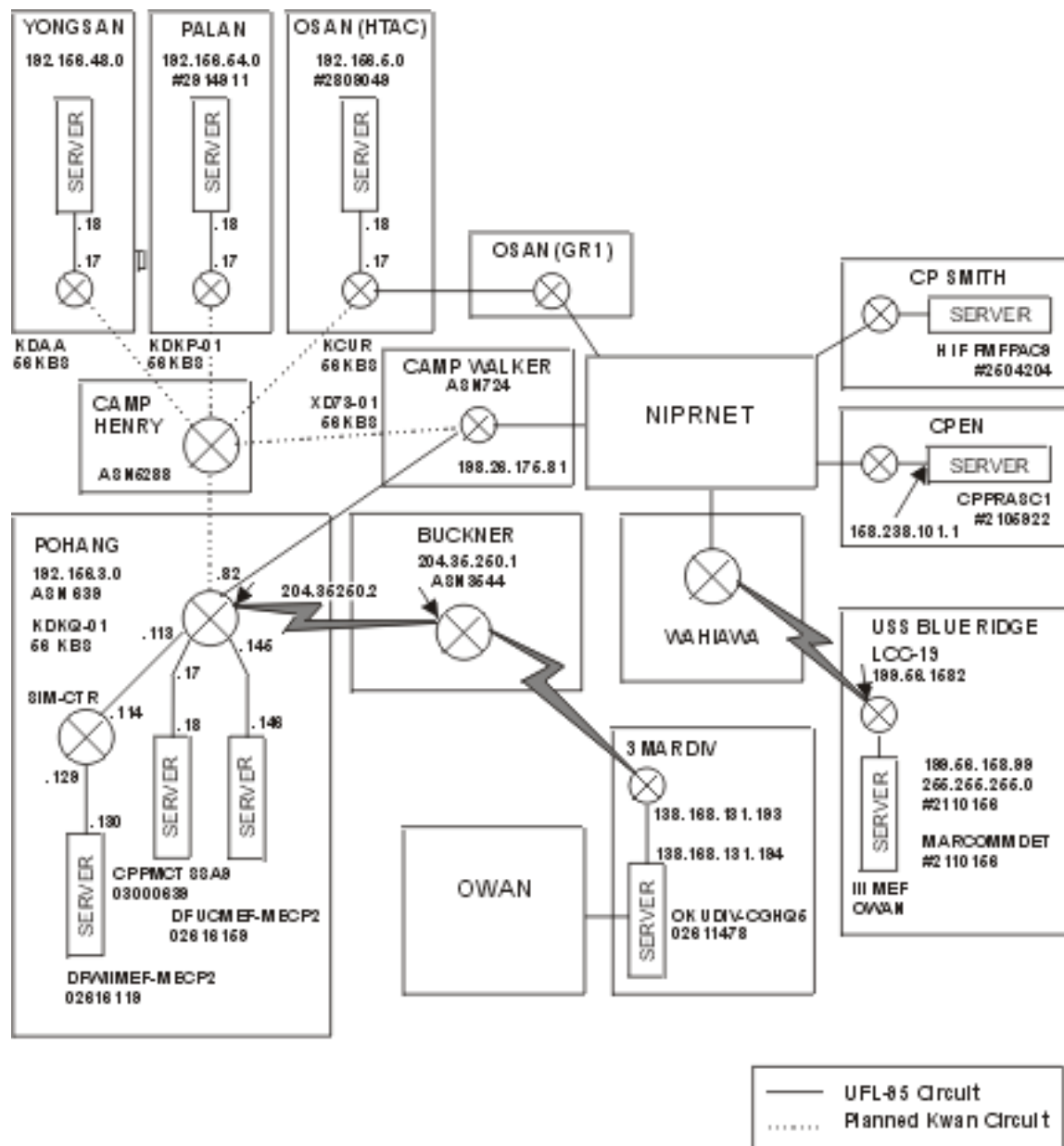


Figure M-2. Sample IP Network Diagram.

(reverse blank)

Appendix N

Points of Contact

Headquarters, United States Marine Corps (C4I)
<http://www.usmc.mil>
DSN 327-5561
Commercial (703) 607-5538

Marine Corps Network Operations Center
Help Desk
<http://www.noc.usmc.mil>
DSN 278-5300
Commercial (703) 784-5300

Architecture Branch
Requirements Division
Marine Corps Combat Development Command
<http://www.archvision.quantico.usmc.mil>
DSN 278-6049
Commercial (703) 784-6049

Marine Corps Systems Command
C4I Directorate, Code CCR, MCHS
<http://www.marcorsyscom.usmc.mil>
DSN 278-5610
Commercial (703) 784-5610

(This WWW site has links to the following:

Marine Corps *Computer Buyer's Guide*
DII COE
MARCORSYSCOM
DefenseLINK
MarineLINK)

Doctrine Division, MCCDC
<http://www.doctrine.quantico.usmc.mil>
DSN 278-6229/33 (Unclassified)
fax x-2917
Commercial (703) 784-xxxx

Command and Control Systems School
Marine Corps University
<http://www.ccss.quantico.usmc.mil>
DSN 278-2438
Commercial (703) 784-2438

Marine Corps Communications Electronics School
MCAGCC
DSN 957-3707 (Ops)

Marine Corps Tactical Systems Support Activity
<http://www.mctssa.usmc.mil>
DSN 365-2167
Commercial (760) 725-2167

National Telecommunications and Information
Administration
Department of Commerce
(Frequency Management-Emission Designator
Codes)
<http://www.ntia.doc.gov>

Naval In-Service Engineering Activity-East
(INFOSEC)
E-mail Questions@infosec.nosc.mil
<http://infosec.nosc.mil>
DSN 563-8878/8879
Commercial 800-304-4636/800-974-5426

Naval Computer Incident Response Team
(NAVCIRT) Hotline
NAVCIRT NIPRNET
E-mail NAVCIRT@fiwc.navy.mil
Commercial 888-NAVCIRT/800-628-8893

(reverse blank)

Appendix O

Glossary

Section I. Acronyms and Abbreviations

AAAV	advanced amphibious assault vehicle	BDA	battle damage assessment
AAV	assault amphibious vehicle	BGLCSS	Battle Group Logistics Coordinated Support System
AAW	antiair warfare	BGIXS	Battle Group Information Exchange System
ACE	aviation combat element	BGP	border gateway protocol
ACI	air combat intelligence	BGPHEs	Battle Group Passive Horizon Extension System
ACOM	Atlantic Command	BLT	battalion landing team
ACP	Allied Communications Publication	Bn	battalion
AC/S	assistant chief of staff	bps	bits per second
ADCP	air defense communications platform	BUU	basic user unit
ADF	automatic direction finding		
ADNS	Automated Digital Network System	C2	command and control
ADP	automated data processing	C3	command, control and communications
AFATDS	Advanced Field Artillery Tactical Data System	C3I	command, control, communications, and intelligence
AFFOR	Air Force Forces	C4	command, control, communications, and computers
AIS	automated information system	C4I	command, control, communications, computers and intelligence
ALICE	all-purpose lightweight individual carrying equipment	CAIMS	Conventional Ammunition Integrated Management System
AM	amplitude modulation	CATF	commander, amphibious task force
ANCD	automated net control device	CBIRF	Chemical/Biological Incident Response Force
ANGLICO	air/naval gunfire liaison company	CCIR	commander's critical information requirements
AO	area of operations	CCR	common computer resources
AOC	air operations center (USAF)	CDE	common desktop environment
AOI	area of interest	CD	compact disk
AOR	area of responsibility	CD-ROM	compact disk-read only memory
ARFOR	Army Forces	CE	command element
ASIP	advanced systems improvement program	CENTCOM	Central Command
ATC	air traffic control	CEOI	communications-electronics operating instructions
ATDL	Army tactical data link	CFC	Combined Forces Command
ATF	amphibious task force	CG	commanding general;
ATFIC	ATF intelligence center		
ATLASS	Asset Tracking Logistics and Supply System		
ATM	asynchronous transfer mode		
ATO	air tasking order		
AUI	autonomous unit interface		
AUTODIN	Automatic Digital Network		
AWACS	airborne warning and control system		

	guided missile cruiser	ConEx	Container Express
CGS.....	common ground station	CONPLAN.....	concept plan
CHBDL.....	common high-bandwidth data link	CONUS.....	continental United States
CI	counterintelligence	COP.....	common operational picture
CIC.....	combat intelligence center	COTS	commercial off the shelf
CINC.....	commander in chief	CP.....	command post
CINCNORAD.....	Commander in Chief, North American Aerospace Defense Command	CPOG.....	chemical protective overgarment
CIS	communications and information systems	CPU.....	central processing unit
CISC.....	complex instruction set computing	CRC	control and reporting center
CISCO.....	Cisco Systems (a computer company)	CRITICOMM	critical communications
CISO	communications information systems officer	C/S	chief of staff
CJCS	Chairman of the Joint Chiefs of Staff	CSDTS	common shipboard data terminal set
CJCSI.....	Chairman of the Joint Chiefs of Staff instruction	CSMA/CD	carrier sense multiple access with collision detection
CJCSM.....	Chairman of the Joint Chiefs of Staff manual	CSR-TEP	circuit switch routing-task execution plan
CJTF.....	commander, joint task force	CSS	combat service support
CLF	commander, landing force	CSSE.....	combat service support element
CMD	command	CSSOC.....	combat service support operations center
CMS	communications security material system	CSU.....	channel service unit
COA	course of action	CTAPS	contingency theater automated planning system
COC	combat operations center	CTT.....	commander's tactical terminal
CODEC	coder-decoder	CUDIXS.....	common user digital information exchange system
COE	common operating environment	CV.....	aircraft carrier
COE-V ...	common operating environment-variant	CVN	aircraft carrier, nuclear
COG	center of gravity	CVSD.....	continuously variable slope delta
COMINT.....	communications intelligence comm		
COMMARFOR	commander, Marine Corps forces	DACT.....	data automated communications terminal
COMMARFORLANT.....	Commander, Marine Corps Forces, Atlantic	DAMA	demand assigned multiple access
COMMARFORPAC.....	Commander, Marine Corps Forces, Pacific	DARPA.....	Defense Advanced Research Projects Agency
COMMARFORRES	Commander, Marine Corps Forces Reserve	DAS	direct access service
COMMARLOGBASES.....	Commander, Marine Corps Logistics Bases	DASC.....	direct air support center
COMM BN	communications battalion	DASC(A)	direct air support center (airborne)
COMM COORD.....	communications coordinator	DAT	digital audio tape
COMNAVFOR	Commander, Navy Forces	DATACOMM.....	data communications
COMPHIBGRU ...	commander, amphibious group	dBm.....	decibels referred to 1 milliwatt; decibel millivolts
COMPUSEC	computer security	DCE	distributed computing environment
COMSEC	communications security	DCN	Data Link Coordination Net
		DCO	dial central office
		DCS.....	Defense Communications System

DCT	digital communications terminal	ESM	electronic warfare support measures
DD	destroyer	EUCE	end user computer equipment
DDG	destroyer	EW	electronic warfare; early warning
DDN	Defense Data Network	EW/C	early warning/control
DEERS	Defense Eligibility Enrollment Reporting System	EWCC	electronic warfare coordination center
DEUCE	downsized end-user computing equipment	F	flash
DF	direction finding	FACP	forward air control post
DII	defense information infrastructure	FAD	fighter air direction
DISA	Defense Information Systems Agency	FAPES	Force Augmentation Planning and Execution System
DISN	Defense Information Systems Network	fax	facsimile
DLTU	digital line termination unit	FDC	fire direction center
DMR	digital modular radio	FDDI	fiber distributed data interface
DMS	Defense Message System	FFCC	force fires coordination center
DNS	Domain Name System	FFIR	friendly force information requirement
DNVT	digital nonsecure voice terminal	FIWC	Fleet Information Warfare Center
DOD	Department of Defense	FLTSAT	fleet satellite
DODD	DOD directive	FLTSATCOM	fleet satellite communications
DODIIS	DOD Intelligence Information System	FLTSEVOCOM	fleet secure voice communications
DON	Department of the Navy	FM	frequency modulation
DSCS	Defense Satellite Communications System	FMF	Fleet Marine Force
DSN	Defense Switched Network	FMFM	Fleet Marine Force manual
DSSCS	Defense Special Security Communi- cations System	FO	Flash Override
DSU	data service unit	FSC2S	Fire Support Command and Control System
DSVT	digital subscriber voice terminal	FSCC	fire support coordination center
DTC	digital technical control	FSK	frequency shiftkey(ing)
DTD	data transfer device	FSSG	force service support group
DTE	data terminal equipment	ft.	foot; feet
DTG	digital transmission group		
DWTS	Digital Wideband Transmission System		
		GARC	GCCS ATO review
EA	electronic attack	GB	gigabite
EAF	expeditionary airfield	GBDL	ground-based data link
EEFI	essential elements of friendly information	GBNP	Global Block Numbering Plan
e.g.	for example	GBS	Global Broadcast System
EGP	exterior gateway protocol	GCA	ground controlled approach
EHF	extremely high frequency	GCCS	Global Command and Control System
ELINT	electronic intelligence	GCE	ground combat element
EMCON	emission control	GCS	ground control station
EMI	electromagnetic interference	GCSS	Global Combat Support System
EP	electronic protection	GENSER	general service (message)
EPLRS	enhanced position location reporting system	GHz	gigahertz
		GMF	ground mobile forces
		GOTS	government off the shelf

GPS	global positioning system	INFOSEC	information security
GPSIU	global positioning system interface units	INMARSAT	international maritime satellite
GSORTS	Global Status of Resources and Training System	INSCOM	U.S. Army Intelligence and Security Command
GTN	Global Transportation Network	INTELINK	intelligence link
GUI	graphical user interface	INTELINK-S	intelligence link-Secret
		I/O	input/output
H&S	headquarters and service	IP	internet protocol
HAVE QUICK	jam-resistant UHF radio	IPA	imagery product archive
HAZMAT	hazardous materials	IPB	intelligence preparation of the battlespace
HD	helicopter direction	IRM	information resource manager
HDC	helicopter direction center	ISC	information systems coordinator
HDLC	high-level data link control	ISMO	information systems management officer
HF	high frequency	ISO	International Organization for Standardization
HFRG	high frequency radio group	IT-21	information technology for the 21st century
HLZ	helicopter landing zone	ITP	integrated terminal program
heavy HMMWV	heavy variant, high-mobility, multipurpose wheeled vehicle	ITSDN	Integrated Tactical-Strategic Data Network
HMMWV ...	high mobility multipurpose wheeled vehicle	ITU	International Telecommunications Union
HPS	high-performance server	IW	information warfare
HPW ...	high-performance workstation/application server	IWF	inter-working function
HQ	headquarters		
HQMC	Headquarters, Marine Corps	JANAP	Joint Army, Navy, Air Force publication
HR	helicopter request	JBS	Joint Broadcast Service
HUMINT	human intelligence	JCCC	joint communications control center
Hz	hertz	JCSE	joint communications support element
		JDISS	Joint Deployable Intelligence Support System
I	immediate	JEPES	Joint Engineer Planning and Execution System
IAS	intelligence analysis system	JFACC	joint force air component commander
IBS	integrated broadcast service	JFC	joint force commander
ICN	idle channel noise	JFLCC	joint force land component commander
ID	identification	JFMCC	joint force maritime component commander
IDNX	integrated digital network exchange		
i.e.	that is	JIEO	Joint Interoperability Engineering Organization
IEEE	Institute of Electrical and Electronic Engineers	JMCIS	Joint Maritime Command Information System
IFF	identification, friend or foe	JMCOMS	Joint Maritime Communications System
IFSAS	interim fire support automated system		
IGRP	interior routing and encapsulation protocol		
IMRAS	Individual Manpower Requirements and Availability System		

JMTCSS Joint Maritime Tactical Communications Switching System	LPD amphibious transport dock
JNAV JOPEs Navigation	LPH amphibious assault ship
JOPEs Joint Operation Planning and Execution System	LSB logistic support base; landing support battalion
JSIPS Joint Services Imagery Processing System	LSD dock landing ship
JSIPS-N JSIPS-Navy	LZ landing zone
JSOTF joint special operations task force	LZCT landing zone control team
JSTARS joint surveillance target attack radar system	m meter
JTF joint task force	MACCS Marine air command and control system
JTIDS Joint Tactical Information Distribution System	MACG Marine air control group
JTT joint tactical terminal	MACS Marine air control squadron
JULLES Joint Universal Lessons Learned System	MAFC MAGTF all-source fusion center
JWICS Joint Worldwide Intelligence Communications System	MAG Marine aircraft group
	MAGTF Marine air-ground task force
	MAGTF II Marine air-ground task force II
	MALS Marine Aviation Logistics Squadron
	MARCOMDET Marine communications detachments
kbps kilobits per second	MARCORMATCOM Marine Corps Material Command
kHz kilohertz	MARCORSYSCOM Marine Corps Systems Command
km kilometer	
LAAD low altitude air defense	MARDIV Marine Division
LAAM light antiaircraft missile	MARFOR Marine Corps forces
LAN local area network	MARFORLANT ... Marine Corps Forces, Atlantic
LAR light armored reconnaissance	MARFORPAC Marine Corps Forces, Pacific
LAV light armored vehicle	MARFORRES Marine Corps Forces Reserve
LCAC landing craft air cushion	MASS Marine air support squadron
LCC amphibious command ship	MATCD Marine air traffic control detachment
LCU landing craft, utility	MAW Marine aircraft wing
LDR low data rate	Mb megabyte
LFOC landing force operations center	Mbps megabits per second
LFSP landing force support party	MCAGCC Marine Corps Air-Ground Combat Center
LGM loop group multiplexer	MCCC Marine Corps Command Center
LHA general purpose amphibious assault ship	MCCDC Marine Corps Combat Development Command
LHD general purpose amphibious assault ship (with internal dock)	MCDP Marine Corps doctrinal publication
LOGAIS logistics automated information system	MCHS Marine common hardware suite
LOG IR Plan Logistics Information Resources Plan	MCIXS ... maritime cellular information exchange system
LOGSAFE logistics sustainment analysis and feasibility estimator	MCMO MEF COMSEC Management Office
	MCO Marine Corps order
	MCPP Marine Corps Planning Process

MCR.....	multichannel radio	MS.....	message switch; Microsoft
MCRP.....	Marine Corps reference publication	MSC.....	major subordinate command
MCTSSA.....	Marine Corps Tactical Systems Support Activity	MS-DOS.....	MicroSoft-disk operating system
MCWP.....	Marine Corps warfighting publication	MSE.....	mobile subscriber equipment
MD.....	medical	MTACCS.....	Marine tactical command and control sections
MDL.....	MAGTF Data Library	MT Bn.....	motor transport battalion
MDR.....	medium data rate	MTF.....	message text format
MDS.....	Message Dissemination System	MTS.....	Marine tactical systems
MDSS II.....	MAGTF Deployment Support System II	MUX.....	multiplex
MECDL.....	mission equipment control data link	MWCS ...	Marine wing communications squadron
MED BN.....	medical battalion	MWSG.....	Marine wing support group
MEDEVAC.....	medical evacuation	MWSS.....	Marine wing support squadron
MEF.....	Marine expeditionary force	NADGE.....	NATO air defense ground environment
MEF (Fwd).....	Marine expeditionary force (forward)	NALCOMIS.....	Naval Aviation Logistics Com- mand Management Information System
MEPES.....	Medical Planning and Execution System	NATO.....	North Atlantic Treaty Organization
METOC.....	meteorological and oceanographic	NAVCIRT.....	Naval Computer Incident Response Team
MEU.....	Marine expeditionary unit	NAVFOR.....	Navy Forces
MEU(SOC)	Marine expeditionary unit (special operations capable)	NAVMACS II.....	Naval Modular Automated Communications Subsystem II
MEWSS.....	Mobile Electronic Warfare Support System	NBC.....	nuclear, biological, and chemical
mHz.....	megahertz	NCIS.....	Naval Criminal Investigative Service
MILSATCOM.....	Military Satellite Communications	NCS-E(D).....	Net Control Station-EPLRS (Downsized)
Milstar.....	military strategic and tactical relay system	NCTAMS.....	naval computer and telecommu- nications area master station
MilVan.....	Military Van	NDI.....	nondevelopmental item
MIME.....	multipurpose internet mail extension	NDP.....	naval doctrine publication
MIMMS.....	Marine Integrated Maintenance Management System	NECC.....	Navy EHF communications controller
MLC.....	Marine Logistics Command	NGF.....	naval gunfire
MLG.....	Marine Liaison Group	NIPRNET.....	nonsecure internet protocol router network
MOE.....	measures of effectiveness	NIPS.....	Naval Intelligence Processing System
MOU.....	memorandum of understanding	NIST.....	National Institute of Standards and Technology
MOOTW.....	military operations other than war	NITF.....	national imagery transmission format
MOS.....	military occupational specialty	NLT.....	not later than
MP.....	military police	NOC.....	network operations center
MPF.....	maritime prepositioning force	nos.....	numbers
MPS.....	maritime prepositioning ships	NRZ.....	nonreturn to zero
MRE.....	meal, ready to eat	NST.....	Navy standard terminal
MRMS.....	Maintenance Resource Management System		

NSTISSI.....	National Security Telecommuni- cations and Information Systems Security Instruction	PLA.....	plain language address
NSW.....	nonsecure warning	PLAD.....	plain language address directory
NTCS-A.....	Navy Tactical Command System- Afloat	PLGR.....	precise lightweight GPS receiver
NTCSS.....	Naval Tactical Command Support System	PLI.....	position location information
NT DII COE.....	nodal terminal defense information infrastructure common operating environment	PLIS.....	Position Location Information System
NTIA.....	National Telecommunications and Information Administration	PLRS.....	Position Location Reporting System
NTP.....	naval tactical publication	POTS.....	plain old telephone system
NTS.....	naval telecommunications system	ppm.....	pulse position modulation
OCAC.....	operations control and analysis center	PPP.....	point-to-point protocol
OEO.....	other expeditionary operations	PR.....	primary zone
OMFTS.....	operational maneuver from the sea	QuadCon.....	Quadruple Container
OPCON.....	operational control	R.....	routine
OPLAN.....	operation plan	RadBn.....	radio battalion
OPNAVINST.....	Chief of Naval Operations Instruction	RAM.....	random access memory
OPORD.....	operation order	RBECS.....	Revised Battlefield Electronic CEOI System
ops.....	operations	RCU.....	remote control unit
OPSEC.....	operations security	RDA.....	Requirement Development Analysis
OPT.....	operational planning team	RECON OPS.....	reconnaissance operations
OSCC.....	operational systems control center	RED.....	record of emergency data regt.....
OSPF.....	open shortest path first	regt.....	regiment
OTCIXS.....	Officer in Tactical Command Information Exchange System	RF.....	radio frequency
OTH.....	over the horizon	RISC.....	reduced instruction set computing
P.....	priority	RLT.....	regimental landing team
PACOM.....	Pacific Command	RMC.....	remote multiplexer combiner
PAL.....	preaffiliation list	RPC.....	remote procedure call
PAO.....	public affairs officer/office	RRT.....	radio reconnaissance team
PC.....	personal computer	RSINISS.....	Revised SINCGARS integrated COMSEC module, nonintegrated COMSEC module support software
PCMCIA.....	Personal Computer Memory Card International Association	SABER.....	situational awareness beacon with reply
PCMT.....	personal computer message terminal	SABRS.....	Standard Accounting, Budgeting, and Reporting System
PDR.....	predefined reports	SACC.....	supporting arms coordination center
PHIBRON.....	amphibious squadron	SADL.....	Situational Awareness Data Link
PIN.....	personal identification number	SAM.....	surface-to-air missile
PIP.....	product improvement program	SAR.....	search and rescue
PIR.....	priority intelligence requirement	SARC.....	surveillance and reconnaissance center
		SASS.....	supporting arms special staff
		SASSY.....	Supported Activities Supply System
		SATCOM.....	satellite communications
		SAW.....	standard application workstation
		SBB.....	switched backbone

SCAMP	sensor control and management platoon	SSU	SIGINT support unit
SCI	sensitive compartmented information	STANAG	standardization agreement
SCR	single-channel radio	STAR-T	Super High Frequency Tri-Band Advanced Range Extension Terminal
SCSI	small computer system interface	STEP	standard tactical entry point
SECNAVINST.	Secretary of the Navy instruction	STOM	ship-to-objective maneuver
SECTEL	secure telephone	STU-III.....	secure telephone unit-type III
SES.....	sensor employment squad	SUADPS	Shipboard Uniform Automated Data Processing System
SGT MAJ	sergeant major	SYSCON.....	systems control
SHF	super high frequency		
SI.....	special intelligence	TAC	tactical
SIDS.....	secondary imagery dissemination system	TACAN.....	tactical air navigation
SIGINT	signals intelligence	TACC.....	tactical air command center
SINCGARS.....	single-channel ground and airborne radio system	TACC(A)	tactical air control center (afloat)
SIP.....	systems improvement program	TACFIRE.....	tactical fire
SIPRNET	secret internet protocol router network	TACINTEL.....	tactical intelligence
SJA.....	staff judge advocate	TACLOG	tactical-logistical group
SL.....	switch locator	TACO II.....	Tactical Communications Protocol
SLCP.....	Ship's Loading and Characteristics Pamphlet	TACON.....	tactical control
SLRP	survey, liaison, and reconnaissance party	TACP	tactical air control party
S&M.....	scheduling and movement	TACSAT	tactical satellite
SMART-T	Secure Mobile Anti-Jam Reliable Tactical Terminal	TAD	tactical air direction
SMTP	simple mail transfer protocol	TADC.....	tactical air direction center
SMU	smart multiplexing unit	TADIL	tactical digital information link
SNAP	Shipboard Nontactical ADP Program	TADIXS A/B	Tactical Data Information Exchange System-Subsystem A/B
SNAPIII	Shipboard Nontactical ADP Program III	TAOC.....	tactical air operations center
SNMP.....	simple network management protocol	TAOM.....	tactical air operations module
SOA	sustained operations ashore	TAR	tactical air request
SOCOM	Southern Command	TARGET.....	Theater Analysis and Replanning Graphical Execution Toolkit
SOP	standing operating procedure	TASS.....	tactical automated switching system
SPE.....	systems planning and engineering	TATC	tactical air traffic control
SPEED	system planning, engineering, and evaluation device	TBM.....	theater ballistic missile
SPMAGTF	special purpose MAGTF	TBMCS	theater battle management core system
Sqdn	squadron	TCAC.....	technical control and analysis center
SRO.....	sensitive reconnaissance operations	TCAC PIP.....	tactical control and analysis center product improvement program
SSCC.....	special security communications central	TCAE	Army Technical Control and Analysis Element
SSCT	special security communications team	TC-AIMS	Transportation Coordinators' Automated Information for Movement System
SSES	ship's signals exploitation space	TCC.....	tactical communications center
SSN	social security number		
SSO	special security officer		

TCIM	tactical communications interface module	TSN	track supervision net
TCO	tactical combat operations	TSO	telecommunications service order
TCP	transmission control protocol	TSR	telecommunications service request
TDBM	technical database management	TTP	tactics, techniques, and procedures
TDDS	Tactical Receive Equipment and Related Applications Program Data Dissemination	UAV	unmanned aerial vehicle
TDMA	time division multiple access	UHF	ultrahigh frequency
TDN	tactical data network	ULCS	unit-level circuit switch
TDS	tactical data system	UNC	United Nations Command
TECHCON	technical control	UNIX	an open-architecture operating system
TELNET	telecommunications network	UPS	uninterruptible power supply
TERPES	Tactical Electronic Reconnaissance Processing and Evaluation System	URL	uniform resource locator
TIBS	tactical intelligence broadcast service	USA	United States Army
TM	technical manual	USAF	United States Air Force
TMIP	Theater Medical Information Program	USMC	United States Marine Corps
TNAPS+	Tactical Network Analysis and Planning System Plus	USN	United States Navy
T/O	table of organization	USTRANSCOM	U.S. Transportation Command
TOW	tube-launched, optically tracked, wire-command link guided missile	VHF	very high frequency
TPFDD	time-phased force and deployment data	VIXS	Video Information Exchange System
TRANSEC	transmission security	VMF	variable message format
TRE	tactical receive equipment	VMFA	Marine fighter attack squadron
TRI-TAC	Tri-Service Tactical Communications System	VPN	voice product net
TRIXS	Tactical Reconnaissance Intelligence Exchange	V/STOL	vertical/short takeoff and landing
TRSS	tactical remote sensor system	W	watts
TSCM	technical surveillance countermeasures	WAN	wide area network
		WWW	world wide web
		XO	executive officer

Section II. Definitions

A

Allied Communication Publication 123 (ACP 123)—ACP 123 defines a military messaging standard. Allied nations have agreed to adopt the ACP 123 Military messaging standard to replace the current human-interactive ACP 127 procedures. The ACP 123 standard is based on the open system X.400 message standard, which provides not only the format of the message, but the procedures and services required in its delivery.

Allied Communication Publication 126 (ACP 126)—ACP 126 defines a character-oriented message standard for use in operations with allied forces.

application—A system or problem to which a computer is applied.

asynchronous—Pertaining to an operation that occurs without a regular or predictable time relationship to a specified event.

asynchronous transfer mode (ATM)—A method of digitized data transmission based on fixed-length cells. ATM can carry multiple types of data—text, voice, imagery, and video—at high speeds.

asynchronous transmission—Data transmission in which the instant that each character, or block of characters, begins to be transmitted is arbitrary. However, the time of occurrence of each signal representing a bit within the character or block is predictable.

B

back lobe—Pertaining to a directional antenna, the radiation occurring in a direction 180 degrees from that of the main axis of radiation.

backbone—The high traffic density connectivity portion of any communications network.

bandwidth—The difference between the limiting frequencies of a continuous frequency band expressed in hertz (cycles per second). The term bandwidth is also loosely used to refer to the rate at which data can be transmitted over a given communications circuit. In the latter usage, bandwidth is usually expressed in either kilobits per second (kbps) or megabits per second (Mbps).

baseband—The original band of frequencies produced by a transducer, such as a microphone, telegraph key, or other signal-initiating device, before initial modulation. Baseband describes the signal state before modulation, before multiplexing, following demultiplexing, and following demodulation.

bit error rate—The number of erroneous bits divided by the total number of bits transmitted, received, or processed over some specified period.

bomb—A computer program, generally malicious in nature, hidden within or emulating another program and designed to execute at a specific future time or on the occurrence of a specific event.

C

client-server architecture—A computer networking architecture, client-server defines a software architecture and not a hardware architecture. A client software entity (client) requests a service from a server software entity (server), which in turn fulfills the request. To fulfill the request the server may provide data, perform processing tasks, control a peripheral, or request the services of another server. A client can request services from multiple servers and a server can service

multiple clients. Because clients and servers are software entities, they can reside on the same computer or be on different computers in a network. Servers are designated according to the services provided. A server providing access to communications services would be called a communications server.

collision detection—A method by which a collision is detected on a LAN transmission medium. A collision occurs when more than one simultaneous transmission is attempted on the LAN.

combat information—Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements.

communications—A method or means of conveying information of any kind from one person or place to another. (Joint Pub 1-02).

conditioned diphasé signaling—A robust form of digital baseband signaling employed by TRI-TAC equipment in which bits are encoded in the phase of the signal.

D

data terminal equipment—A networked device, such as a PC, that is capable of transmitting and receiving digital data signals over a communications circuit.

digital backbone—A term loosely applied to the TRI-TAC-based circuit switched communications network employed by the Marine Corps. Used synonymously with switched backbone.

digital signature function—A cryptographic technique for authenticating electronic documents, much as a written signature verifies the au-

thenticity of a paper document. A message is encrypted with the sender's digital private key and the recipient decrypts the signature with the sender's digital public key.

digital switch—A switch that performs time-division multiplexed switching of digitized signals. When used with analog inputs analog-to-digital and digital-to-analog conversions are necessary.

digital transmission—The transmission of a digital bit stream that may include digitized voice or data or both. The transmission signal itself may be either discrete or continuous (analog).

digital transmission group—A group of digitized voice and/or data channels that have been combined (multiplexed) into a single digital bit stream for transmission over communications media.

DISA megacenter—One of several large data processing centers maintained and operated by DISA, such as the Cleveland Center, which supports the Defense Finance and Accounting Service.

domain name—The symbolic name assigned to a host on an IP network. Syntactically the domain name consists of a sequence of names separated by periods. A domain is a logical grouping of IP hosts.

domain name system—The online distributed database system used to relate (map) readable, alphabetic domain names with numeric IP addresses.

double sideband—The transmission of a modulated carrier wave accompanied by both sidebands resulting from modulation. The upper sideband corresponds to the sum of the carrier and modulation frequencies, whereas the lower sideband corresponds to the difference between the carrier and the modulation frequencies.

F

forward lobe—Pertaining to a directional antenna, the radiation occurring along the main axis of radiation.

full duplex—Refers to a mode of transmission in which communication between two terminals takes place in both directions simultaneously.

G

gateway—In a communications network, a network node that is equipped for interfacing with another network that uses different protocols. The term is loosely applied to a computer or computer software configured to perform the tasks of a gateway.

H

half-duplex—Refers to a mode of transmission in which communication between two terminals occurs in either direction, but in only one direction at a time. This is the typical mode of operation for tactical single-channel radios.

host—In a computer network, a computer that provides services to end users. Those services are considered to be hosted on that computer. The term host also refers to the computer on a network that performs network control functions.

I

IDNX—Integrated Digital Network Exchange, or IDNX, devices provide automated link bandwidth management that allocates available circuits as needed. These devices are used at network nodes to allow for a virtual network with automatic routing and rerouting. IDNX devices are easily upgraded to asynchronous transfer mode (ATM) capability.

information system—The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (Joint Pub 1-02)

in-line network encryptor—A cryptographic device that permits the transmission of classified data on unclassified networks or SCI data on secret networks. A key feature of in-line network encryptors is that they only encrypt the data, not the address information. In-line network encryptors, through software configuration and appropriate keying material, may be used to link multiple LANs of one classification level by using a data communications network operating at a lower classification level.

internet—The worldwide interconnection of individual computer networks operated by government, industry, academia, and private parties. The internet was originally developed by the Defense Advanced Research Projects Agency (DARPA) to interconnect laboratories and academic institutions engaged in government-sponsored research.

internet protocol (IP)—A DOD standard protocol designed for use in interconnected systems (internets) of packet-switched communications networks. The IP provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are identified by fixed length addresses (IP addresses).

IP address—A unique numerical address assigned to each host on an IP network based on a standard scheme and by a central agency. Used to communicate between hosts on the network.

isochronous—Pertaining to data transmissions in which the time interval separating two corresponding signal state transitions is equal to the

unit interval of that signal state or a multiple of the unit interval.

J

Joint Army, Navy, Air Force Publication (JANAP)-128 local area network—A joint standard for AUTODIN message formats and procedures. A data communications system that lies within a limited geographic area, has a specific user group, and uses a specific topology. A LAN is not part of a public switched telecommunications network although it may be connected to such a network.

L

loop—A communication channel from a switching center or an individual message distribution point to the user terminal. In a telephone system, a pair of wires running from a central office to a subscriber's telephone.

M

media access method—The method by which a terminal on a LAN accesses the LAN transmission medium.

modem—In computer communications, a device used for converting digital signals into, and recovering them from, quasi-analog signals that are suitable for transmission over analog communications channels.

modulation—The process of varying a characteristic (e.g., frequency, phase, amplitude) of a carrier signal in accordance with an information bearing signal.

multichannel—Pertaining to communications, usually full duplex, on more than one channel si-

multaneously. Multichannel transmission may be accomplished by time-, frequency-, code-, and phase-division multiplexing, or space diversity.

multiplexer—A device that combines (multiplexes) multiple input signals (information channels) into an aggregate signal (common channel) for transmission.

multipurpose internet mail extension (MIME)—MIME is the internet standard protocol for sending multipart, multimedia, and binary data by using e-mail. Typical uses of MIME include sending images, audio, word processing documents, programs, or even plain text files when it is important that the mail system does not modify any part of the file. MIME also allows for labeling message parts so that a recipient (or mail program) may determine what to do with them. The MIME internet standard is described in RFC-1521.

O

open systems—A system with characteristics that comply with specific, publicly maintained (rather than proprietary), readily available standards. Such a system, by virtue of adherence to the standard, may be connected to other systems that comply with those same standards.

order wire—An auxiliary circuit or channel for use by operating and/or maintenance personnel for communications incident to establishing, operating, maintaining, and controlling communications facilities, systems and equipment.

P

packet switch—A switch that breaks messages into data packets for transmission over a network and reassembles data packets into messages upon receipt.

protocol—A formal set of specifications governing the format and control of interaction among terminals communicating over a network.

R

radio-wire integration—The combining of wire circuits with radio functions.

relational database—A database that is based on the relational model. The relational model relies on the mathematics of set theory, thereby providing a solid theoretical base for the management of data. Relational databases are typically easier to use and maintain than nonrelational databases. The relational model provides for improved data availability, data integrity, and data security because the model rigorously defines these features as part of the database, not as part of the processes that maintain the database.

repeater—A device that amplifies, reshapes, re-times or performs a combination of these functions on an input signal for retransmission. The input signal may be either analog or digital. Repeaters are used to extend the distance that network signals can be transmitted.

request for comment (RFC)—A document used by the Internet Activities Board (the governing body for internet protocols) to develop and to configuration manage internet protocols.

router—A device used to interconnect two or more data communication networks. The router reads the network address of all data packets and forwards to the addressee via the best available communications path.

S

simple mail transfer protocol (SMTP)—The internet standard protocol used to facilitate the exchange of e-mail across an internet. SMTP

establishes a link to a remote host and handles the translation of different mail file formats between hosts. To arrange for mail delivery, e-mail applications running on a particular host must make a call to SMTP which then handles the delivery. SMTP uses internet domain names to find a connection, relying on the DNS to make the translations to IP numeric addresses.

simple network management protocol (SNMP)—The internet standard protocol used to provide the network management capabilities needed to monitor and control a network.

simplex—Refers to a mode of operation in which communication between two terminals can take place in only one direction.

single sideband—A mode of communications in which the carrier wave and one sideband are suppressed. Single sideband operation requires less power at the transmitter for the same effective signal at the receiver, a narrower frequency band can be used, and the signal is less affected by selective fading or interference.

skywave—A radio wave that reaches the receiving location after refraction from the ionosphere.

synchronous—Pertaining to an operation that occurs with a regular or predictable time relationship to a specified event.

systems network architecture (SNA)—A proprietary network architecture developed by IBM.

T

T1 circuit—A communications circuit providing 1.544 Mbps capacity.

TELNET—The internet standard virtual terminal protocol that is used for remote terminal connection service. TELNET allows a remote terminal to

login to and access services from a host computer by using dial-in or other network connections.

timing—The synchronization of communications signals. Of critical importance for digital communications networks and for secure communications.

token—A bit pattern used in the token ring and token bus media access methods for controlling access to the medium.

topology—In the context of a communications network, the term topology refers to the way in which the stations or terminals attached to the network are interconnected. The common topologies for local area networks are the star, ring, and bus.

transponder—**1.** An automatic device that receives, amplifies, and retransmits a signal on a different frequency. **2.** An automatic device that transmits a predetermined message in response to a predefined received signal. (Note: Examples of transponders are identification, friend or foe (IFF) systems and air-traffic-control secondary radar (beacon radar) systems.) **3.** A receiver-transmitter which will generate a reply signal upon proper interrogation. (Joint Pub 1-02) **4.** Device in a communications satellite that receives a signal from a sending earth station and retransmits the signal to one or more receiving earth stations.

Trojan horse—A computer program containing an apparently or actually useful function that also contains hidden functions that allow unauthorized collection, falsification, or destruction of data.

trunk—A trunk is a single circuit between two switching centers or individual message distribution points. This is in contrast to a loop, which is a single circuit between the switching center or message distribution point and the individual subscriber terminal. A trunk group is formed by two or more trunks between the same two points.

trusted workstation—A workstation that meets strict security accreditation standards and is considered secure from exploitation.

V

virus—A self-replicating malici attaches itself to an application program or other executable system component.

W

wide area network—A term loosely applied to any communications network extending over a large geographic area.

worm—An independent computer program designed to self-replicate from computer to computer across computer networks often clogging networks and monopolizing computer system resources as it spreads.

X

X.400—Open system standard for e-mail.

X.500—Open system standard for network directory service.

X.509 certificate—Open system standard for security. Many internet protocols and applications employ public-key technology for security purposes and require a public-key infrastructure to securely manage public keys for widely-distributed users or systems. The X.509 standard provides basis for such an infrastructure, defining data formats and procedures related to distribution of public keys via certificates digitally signed by certification authorities.

(reverse blank)

Appendix P

References and Related Publications

Standardized Agreements (STANAGs)

4206	The NATO Multi-Channel Tactical Digital Gateway—System Standards
4207	The NATO Multi-Channel Tactical Digital Gateway—Multiplex Group Framing Standards
4208	The NATO Multi-Channel Tactical Digital Gateway—Signalling Standards
4209	The NATO Multi-Channel Tactical Digital Gateway—Standards for Analogue to Digital Conversion of Speech Signals
4210	The NATO Multi-Channel Tactical Digital Gateway—Cable Link Standards
4211	The NATO Multi-Channel Tactical Digital Gateway—System Control Standards
4212	The NATO Multi-Channel Tactical Digital Gateway—Radio Relay Link Standards
4213	The NATO Multi-Channel Tactical Digital Gateway—Data Transmission Standards
5040	NATO Automatic and Semi-Automatic Interfaces Between the National Switched Telecommunications Systems of the Combat Zone and Between These Systems and the NATO Integrated Communications System (NCIS)—For the Period 1979 to the 1990s

Allied Communications Publications (ACPs)

121	Communications Instructions—General
122	Series Communications Instructions—Security
123	Common Messaging Strategy and Procedures
126	Communications Instructions Teletypewriter Procedures
167	Series Glossary of Communications-Electronics Terms

Department of Defense Publications

Directives (DODDs)

5200.1	Information Security Program
5200.28	Security Requirements for Automated Information Systems (AISs)
8320.1	DOD Data Administration

Instruction (DODI)

4630.8	Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C3I) Systems
--------	--

Chairman, Joint Chiefs of Staff (CJCS) Publications

Joint Publications (Joint Pubs)

0-2	Unified Action Armed Forces (UNAAF)
1-0	DOD Dictionary of Military and Associated Terms
3-0	Doctrine for Joint Operations
5-0	Doctrine for Planning Joint Operations
5-03.1	Joint Operation Planning and Execution System—Volume 1
6-0	Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations
6-02	Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems
6-02.1	Joint Connectivity Handbook

Manuals (CJCSMs)

6231.01A	Manual for Employing Joint Tactical Communications—Joint Tactical Systems Management
6231.02	Manual for Employing Joint Tactical Communications—Joint Voice Communications Systems
6231.03A	Manual for Employing Joint Tactical Communications—Joint Data Systems
6231.04	Manual for Employing Joint Tactical Communications—Joint Transmission Systems
6231.05	Manual for Employing Joint Tactical Communications—Joint Communications Security
6231.06	Manual for Employing Joint Tactical Communications—Joint Technical Control Procedures and Systems
6231.07A	Manual for Employing Joint Tactical Communications—Joint Network Management and Control

Instructions (CJCSIs)

6110.01	CJCS-Controlled Tactical Communications Assets
6230.03	Communications-Electronics Operation Instructions/Signal Operation Instructions

Joint Army, Navy, Air Force Publications (JANAPs)

128	Automatic Digital Network (AUTODIN) Operating Procedures
137	Automatic Voice Network (AUTOVON) Operating Procedures

Army Publications

Field Manuals (FMs)

11-24	Signal Tactical Satellite Company
11-25	Signal Troposcatter Company
11-30	MSE Communications in the Corps/Division
11-32	Combat Net Radio Operations
11-41	Signal Support: Echelons Corps and Below (ECB)
11-43	Signal Leader's Guide
11-50	Combat Communications within the Division (Heavy and Light)
24-2	Spectrum Management
24-11	Tactical Satellite Communications
24-18	Tactical Single-Channel Radio Communications Techniques
24-19	Radio Operator's Handbook
24-26	Tactical Automatic Switching
100-6	Information Operations

Technical Manuals (TMs)

11-5820-890-10-1	Operator's Manual for SINCGARS Ground Combat Net Radio, ICOM Manpack Radio AN/PRC-119A (NSN 5820-01-267-9482) (EIC: L2Q) Short Range Vehicular Radio AN/VRC-87A (5820-01-267-9480) (EIC: L22) Short Range Vehicular Radio with Single Radio Mount AN/VRC-87C (5820-01-304-2045) (EIC: GDC) Short Range Vehicular Radio with Dismount AN/VRC-88A (5820-01-267-9481) (EIC:L23) Short Range Vehicular Radio with Dismount and Single Radio Mount AN/VRC-88C (5820-01-304-2044) (EIC: GDD) Short Range/Long Range Vehicular Radio AN/VRC-89A (5820-01-267-9479) (EIC: L24) Long Range Vehicular Radio AN/VRC-90A (5820-01-268-5105)(EIC:L25) Short Range/Long Range Vehicular Radio with Dismount AN/VRC-91A (5820-01-267-9478) (EIC: L26) Long Range/Long Range Vehicular Radio AN/VRC-92A (5820-01-267-9477) (EIC: L27)
11-5820-890-10-2	SINCGARS ICOM Ground Radio Operator's Pocket Guide for Manpack Radio AN/PRC-119A (NSN 5820-01-267-9482) (EIC: L2Q) Short Range Vehicular Radio AN/VRC-87A (5820-01-267-9480) (EIC: L22) Short Range Vehicular Radio with Single Radio Mount AN/VRC-87C (5820-01-304-2045) (EIC: GDC) Short Range Vehicular Radio with Dismount AN/VRC-88A (5820-01-267-9481) (EIC: L23) Short Range Vehicular Radio with Dismount and Single Radio Mount AN/VRC-88C (5820-01-304-2044) (EIC: GDD) Short Range/Low Range Vehicular Radio AN/VRC-89A (5820-01-267-9479) (EIC: L24) Long Range Vehicular Radio AN/VRC-90A (5820-01-268-5105) (EIC: L25) Short Range/Long Range Vehicular Radio with Dismount AN/VRC-91A (5820-01-267-9478) (EIC: L26) Long Range/Long Range Vehicular Radio AN/ VRC-92A (5820-01-267-9477) (EIC: L27)
11-5820-890-10-6	SINCGARS ICOM Ground Radios used with Automated Net Control Device (ANCD) AN/CYZ-10 Operator's Pocket Guide Radio Sets Manpack Radio AN/PRC-119A) (NSN: N/A) (EIC: N/A) Vehicular Radios (AN/VRC-87A-C thru AN/VRC-92A) (NSN: N/A) (EIC: N/A)

11-5820-890-10-8 Operator's Manual for SINCGARS Ground Combat Net Radio, ICOM Manpack Radio, AN/PRC-119A (NSN 5820-01-267-9482) (EIC: L2Q), Short Range Vehicular Radio AN/VRC-87A (5820-01-267-9480) (EIC: L22), Short Range Vehicular Radio with Single Radio Mount AN/VRC-87C (5820-01-304-2045) (EIC: GDC), Short Range Vehicular Radio with Dismount AN/VRC-88A (5820-01-267-9481) (EIC: L23), Short Range/Long Range Vehicular Radio AN/VRC-88C (5820-01-304-2044) (EIC: 6DD), Short Range/Long Range Vehicular Radio AN/VRC-89A (5820-01-267-9479) (EIC: L24), Long Range Vehicular Radio AN/VRC-90A (5820-01-268-5105) (EIC: L25), Short Range/Long Range Vehicular Radio with Dismount AN/VRC-91A (5820-01-267-9478) (EIC: L26), Short Range/Long Range Vehicular Radio AN/BRC-92A (5820-01-267-9477)(EIC: L27) used with Automated Net Control Device (ANCD) (AN/CYZ-10) Precision Lightweight GPS Receiver (PLGR) (AN/PSN-11) Secure Telephone Unit (STU) Frequency Hopping Multiplexer (FHMUX)

Navy Publications

Navy Doctrine Publications (NDPs)

5 Naval Planning
6 Naval Command and Control

Navy Warfare Publication (NWP)

4 Basic Operational Communication Doctrine

Navy Technical Publications (NTPs)

3 Telecommunications Users Manual
4 Naval Telecommunications Procedures—Fleet Communications
5 Naval Telecommunications Procedures—Voice Communications
6 Naval Telecommunications Procedures—Spectrum Management Manual

Office of the Chief of Naval Operations Instruction (OPNAVINST)

5510.1H Messages Requiring Special Handling, Information Security Program

Marine Corps Publications

Doctrine Publications (MCDPs)

1 Warfighting
1-1 Strategy
1-2 Campaigning
1-3 Tactics
2 Intelligence
3 Expeditionary Operations
4 Logistics
5 Planning
6 Command and Control

Warfighting Publications (MCWPs)

0-1.1	Componency
2-1	Intelligence Operations
3-1	Ground Combat Operations (in development)
3-2	Aviation Operations (in development)
3-25.5	Direct Air Support Center Handbook
3-25.7	Tactical Air Operations Center Handbook
4-1	Logistics Planning and Operations (in development)
5-1	Marine Corps Planning Process (in development)

Reference Publications (MCRPs)

5-2A	Operational Terms and Graphics
6-22A	TALK II-SINCGARS: Multiservice Communications Procedures for the Single-Channel Ground and Airborne Radio System
6-22B	Multiservice Procedures for Spectrum Management in a Joint Environment
6-22C	Radio Operator's Handbook (in development)
6-22D	Field Antenna Handbook (in development)
6-22E	TTP For The AN/TSQ-1

Orders (MCOs)

1510.83A	Individual Training Standards (ITS)
P3000.18	Marine Corps Planner's Manual
5236.2	ADP Resources Delegation Program Order
5271.4	E-Mail Policy and Guidance
P5510.14	AIS Security Program

Bulletin (MCBul)

3000	Table of MARES Reportable Equipment
------	-------------------------------------

Technical Manuals (TMs)

8B552B-10/1A	Operator's Manual for Multiplexers/Demultiplexers TD-1389(P)(V)1/G (NSN 5895-01-188-8820) (EIC: L2R) TD-1389(P)(V)2/G (5895-01-186-3235) (EIC: L2N)
07748B-12/1	Operational and Organizational Maintenance Instruction for the AN/PRC-104B(V)1, (V)4 Radio Set
07749A/ 07743A-12/2	Operator's and Organizational Maintenance Instruction Amplifier-Converter AM 6879/URC
07508A-14	Instruction Manual Antenna, AS-2259/GR (FSN 5895-106-6130) and Adapter, Antenna to Antenna Base MX-9313/GR (FSN 5985-172-6518)
08347A-10/1	Operator's Manual for Satellite Communications Terminals, AN/TSC-85B(V)1 (NSN 5895-01-284-8305) and AN/TSC-85B(V)2 (5895-01-248-8308)

08347B-12/1-1	Operator's and Organizational Maintenance Manual for Satellite Communications Terminals AN/TSC-85B(V)1 (NSN 5895-01-284-8305) and AN/TSC-85B(V)2 (5895-01-284-8308) Operation and Operator Maintenance
08347B-12/1-2	Operator's and Organizational Maintenance Manual for Satellite Communications Terminal AN/TSC-85B(V)1 (NSN 5895-01-284-8305) (EIC: L3F) and AN/TSC-85B(V)2 (5895-01-284-8308) (EIC: N/A)
08348A-10/1	Operator's Manual for Satellite Communications Terminals AN/TSC-93B(V)1 (NSN 5895-01-284-8306) and AN/TSC-93B(V)2 (5895-01-284-8307)
08348B-12/1-1	Operator's and Organizational Maintenance Manual for Satellite Communications Terminals AN/TSC-93B(V)1 (NSN 5895-01-284-8305) (EIC: L3E) and AN/TSC-93B(V)2 (5895-01-284-8307) (EIC: N/A)
08439A-12/2-1	Operator and Organizational Maintenance Switchboard, Telephone, Automatic, SB-3865(P)/TCC
08440A-12/2-1	Central Office Telephone, Automatic, AN/TTC-42(V)
08467A-10/1	Operator's Manual for Multiplexer, Digital, TD-1337(V)1/G, (NSN 7025-01-112-6311), TD-1337(V)2/G (7025-01-112-6310), TD-1337(V)3/G (7025-01-112-6312), and TD-1337(V)4/G (7025-01-127-7020)
08658A-14/1	Combined Operation and Maintenance Instructions Organizational and Intermediate Radio Terminal Set AN/TRC-170(V)3 Part Number 951100-5 (NSN 5820-01-148-3976)
08761A-12/1	Operator's and Unit Maintenance Manual for Digital Data Modem MD-1026(P)/G (NSN 5820-01-145-4945)
09280A-14&P/1	Microwave Antenna Group OE-468
09543A-14	Operator and Troubleshooting Checklist for the Radio Terminal Set AN/MRC-142
09589A-14&P/1	Communications Central, AN/TSC-120
2000-15/2B	Principal Technical Characteristics of U.S. Marine Corps Communication-Electronic Equipment
4700-15/1	Ground Equipment Record Procedures
5805-12/1	Operator's and Organizational Maintenance Manual for Multiplexer, TD-1235(P)/TTC (NSN 5820-01-145-2460)

5805-12/2 Operator's and Unit Maintenance Manual for Multiplexer, TD-1236/G (NSN 5820-01-145-2461)

10149A- Tactical Combat Operations (TCO) Technical Manual (NSN 5895-01-392-0294)
13&P/1-1

Miscellaneous Publications

Joint Manual of Regulations and Procedures for Federal Radio Frequency Management

Manual for Regulations and Procedures for Federal Radio Frequency Management (also referred to as the NTIA Manual or Redbook) (<http://www.ntia.doc.gov/osmhome/redbook/redbook.html>)

DISA Contingency Plan 10-95

Computer Buyer's Guide (<http://www.marcorsyscom.usmc.mil>)

Ship's Loading and Characteristics Pamphlet